The Practical Byzantine Fault Tolerance Algorithm: Versatile Applications Across Diverse Fields

Yanyan Zhang

School of Internet, Anhui University, Hefei, 230000, China
y02214566@stu.ahu.edu.cn

Abstract. In recent years, the rise of blockchain technology has sparked significant interest in both cybersecurity and financial investment sectors. Blockchains, categorized into permissioned and permissionless types based on their unique attributes, have shown varied applications. Notably, permissioned blockchains are proving to be more relevant for practical implementations than their permissionless counterparts. One critical aspect of blockchain technology is its consensus protocols, which are fundamental to its operation and integrity. This article provides a succinct overview of the Practical Byzantine Fault Tolerance (PBFT) algorithm, a cornerstone in blockchain technology. It also explores three distinct technical implementations of the PBFT algorithm: Hyperledger Fabric, which is renowned for its robust enterprise solutions; HotStuff, known for its scalability and efficiency improvements; and Diem, a blockchain initiative originally started by Facebook, aimed at transforming financial services. Each of these applications demonstrates the versatility and potential of the PBFT algorithm to address specific needs and challenges within various blockchain frameworks.

Keywords: Hyperledger Fabric, Diem, HotStuff, PBFT.

1 Introduction

In recent years, cryptocurrencies like Bitcoin and Ethereum have garnered widespread public attention. Central to these digital currencies is blockchain technology, a revolutionary technical backbone that enables the secure, transparent functioning of digital transactions without the need for centralized oversight. This technology is primarily divided into two categories based on access permissions: permissionless chains and permissioned chains [1]. Due to their enhanced security features and controlled access, permissioned blockchains are increasingly preferred in practical applications across various industries.

This article delves into the specifics of permissioned blockchains and introduces the Practical Byzantine Fault Tolerance (PBFT) algorithm, a pivotal consensus mechanism in blockchain technology that ensures reliability and fault tolerance within the network [2]. The PBFT algorithm is critical for maintaining the consistency and security of the blockchain, making it a fundamental aspect of this technology.

Y. Wang (ed.), *Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024)*, Advances in Computer Science Research 115,
https://doi.org/10.2991/978-94-6463-540-9_31

Furthermore, the article explores three technological implementations that utilize the PBFT algorithm: Hyperledger Fabric, HotStuff, and Diem. Hyperledger Fabric is an open-source enterprise blockchain platform that offers modularity and versatility for various business applications. It is designed for industrial uses where performance, scalability, and levels of trust vary between transactions. HotStuff further refines the approach of PBFT by enhancing its efficiency and scalability, making it suitable for larger networks with higher throughput demands. Lastly, Diem, initiated by Facebook, represents a significant foray into blockchain by a global tech giant, aimed at creating a stable, widely accepted digital currency that could potentially transform global financial systems.

Each of these technologies showcases the flexibility and adaptability of the PBFT algorithm to meet the diverse needs of different blockchain applications, ranging from enterprise solutions to large-scale digital currencies. By focusing on these adaptations, the article highlights the broad potential and applicability of permissioned blockchains in modern digital landscapes, illustrating how foundational blockchain technology is continually evolving to meet the demands of various sectors.

2 Relevant theories

2.1 Definition of Blockchain

Blockchain is a decentralized distributed ledger technology and its core principle lies in the use of cryptography to ensure the security and trustworthiness of data exchange and records [3]. In a blockchain, data grows in blocks and is chronologically chained into a main chain, where each node keeps a complete copy of the ledger and maintains the consistency of the data through a consensus algorithm.

Generally speaking, blockchains are usually classified into two different types: the permissionless chain and the permissioned chain [4]. The main way to distinguish them is that the former is open to anyone while the latter is limited to be participated by affiliate members only. In other words, the users without identificationis is not allowed to access the permissioned blockchain [5]. Due to their different characteristics, this article will focuses on the permissioned blockchain and its related applications.

As is known, a permissioned blockchain is a distributed ledger that can only be accessed by users with permissions, which means that it’s not accessible to everyone. Only when some actions are with the permission of the ledger administrators can the users perform them. Also, it’s worth noting is that the users need to identify themselves before this process.

The permissioned blockchain is able to be implemented in various ways. For instance, some only allow the users with permissions to operate on the module, while the other chains need to be able to connect them and carry out the work. Usually, permissioned blockchains are used for supplying chain management, creating contracts and verifying payments between parties and otherwise [6].

2.2 PBFT Algorithm

The consensus mechanism is the core of blockchain technology. And PBFT is a consensus algorithm commonly used by permissioned blockchains, which was proposed mainly to solve the Byzantine General problem [7].

To put it simply, the Byzantine General problem is a question about the minority obeying the majority. Each fief of the Byzantine Roman Empire had an army under the command of a general and the general could only rely on the messengers to convey information among them. In the times of war, the Byzantine army could win the target only when it had a numerical superiority [8]. However, there may be traitors in the army, and when the enemy forces unite with them and the number of loyal generals is outnumbered, the attack will fail.

The process of PBFT algorithm can be divided into the following steps:

Request: The client sends a request to peer0 in the request phase.

Pre-prepare: After receiving a request from the client, peer0 broadcasts the request in the pre-prepare phase.

Prepare: After receiving the broadcast request, peer1, peer2, and peer3 enter the prepare stage, and broadcast the result of "ready to submit this request" to all other nodes in this stage.

Commit: All nodes, after receiving enough (more than 2/3 of the nodes, including themselves) to broadcast the "Prepare to submit this request" result from other nodes, enter the commit phase and broadcast a "submit this request" result to other nodes [9].

Reply: When a node receives enough (more than 2/3 of the nodes, including themselves) in the commit phase to broadcast the result of "submit this request", it can confirm that the request is consensus, enter the reply phase, and return the result of "request consensus successful" to the client in the reply phase. As shown in Fig 1.

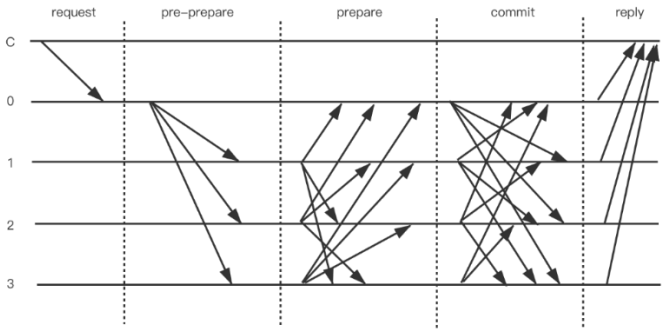

Fig. 1. Flowchart of the PBFT algorithm.

3 System Analysis and Application Research

3.1 Hyperledger Fabric

HyperLedger Fabric is an open source enterprise-level license distributed ledger technology (DLT), which is established under the Linux Foundation. So it's managed by multiple technical memberships and its projects are maintained by people from multiple organizations [10].

One of the most distinctive features of the HyperLedger Fabric is that it's designed to support a pluggable consensus protocol, which allows it to be more efficiently customized to fit specific use cases and trust models.

Moreover, the ledger subsystem of HyperLedger Fabric is composed by two elements: the world state and the transaction log. And everyone participate in it has a copy of the ledger that can be sent to the Hyperledger Fabric network where they belong.

Smart Contact. The smart contracts, which is called chaincode in Hyperledger Fabric, is a trusted distributed application. In most cases, only the world state is able to interact with it while the transaction log is not.

Besides, chaincode can be implemented in various programming languages. For example, it support Go, Node.js, and Java chaincode to write the smart contracts now. Thus, Hyperledger Fabric is the first distributed ledger platform that supports common standard programming languages to write smart contracts, instead of being limited to specific domain languages. This design makes HyperLedger Fabric have great performances in terms of transaction processing and confirmation.

What's more, HyperLedger Fabric introduces a new structure for transactions called execute-order-validate. By dividing the transaction flow into three steps, the problems that would have occurred with the previous model have been optimized. And this kind of design is quite different from the order-execute paradigm, where Fabric executes the transaction before reaching a final agreement on it.

Privacy. About the privacy, Hyperledger Fabric employs an immutable ledger on a per-channel basis, as well as chaincode that can manipulate and modify the current state of assets, such as update key-value pairs. For example, assuming that every participant is operating on the same public channel, then the ledger can be shared across the whole network or privatized to only receive the specified users.

In the latter scenario, the users will create an independent channel so as to segregate their transactions and ledgers. In order to solve the problem that the gap between transparency and privacy is hard to bridge, chaincode can only be installed on peers that is able to perform actions only after accessing the asset situations. In other words, if the chaincode is not installed on the peer, it cannot interact with the ledger in a proper way. Additionally, the Fabric platform now is developing zero-knowledge proofs that can help to improve its privacy functions in the future.

3.2 HotStuff

HotStuff is a Byzantine Fault Tolerant consensus agreement based on the Leader, which is the first consensus algorithm to implement the Linear view change and have Optimistic Responsiveness. The advantage of it lies in the fact that its algorithm implementation complexity is relatively low and it is easy to understand for both the relevant practitioners and the general public. Once network communication becomes synchronized, HotStuff is able to get the right Leader to drive protocol agreement at the speed of actual network latency. And also the complexity of communication will be linearly related to the number of replicas.

Features. One of its features is that HotStuff turns the mesh communication network topology of PBFT into a star one that is, it relies on the Leader for every communication (see Fig.2).

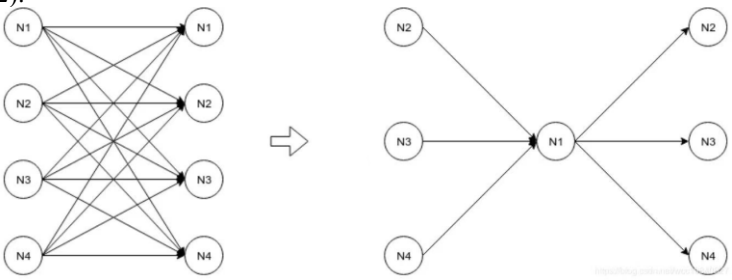

Fig. 2. The change of network topology from a mesh to a star by HotStuff.

What's more, it adopts 3 rounds of 2/3 votes, which includes three stages: precommit, commit and decide. The so-called voting is that other nodes sign a message and send it to the Leader (see Fig.3).

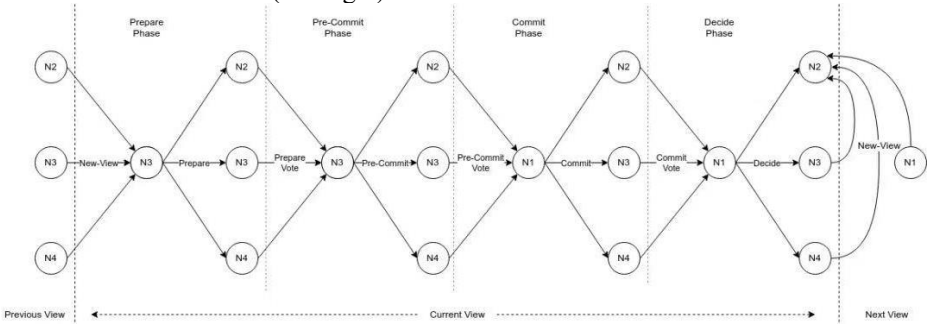

Fig. 3. The 3 rounds of 2/3 votes in HotStuff.

Also, it has the fluidization of the consensus process with the same mechanism as EOS.

3 Rounds of Votes. If there is no order between proposals, then each vote can be for multiple proposals at the same time. For example, if the leader node proposes multiple proposals, the other nodes will vote once in the prepare phase, and this vote will take effect on these proposals at the same time. However, the proposals are sequential. So it need to choose a way like the CPU is executing the instructions. In the same way, the proposal here is also divided into several stages, overlapping the different phases of different proposals (see Fig.4).

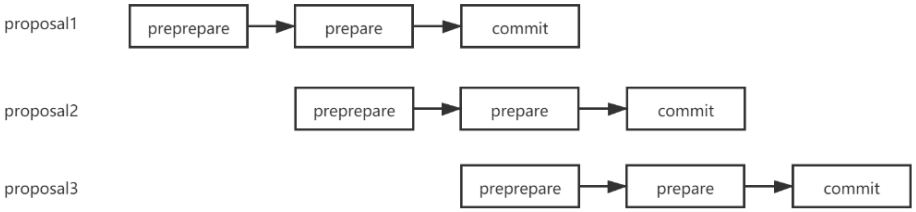

Fig. 4. The execution cycles of different proposals overlap.

Obviously, the execution cycles of different proposals are overlapping the pre-commit, which means that when the Leader receives prepare votes for the current proposal, it will combine them into a prepareQC and then broadcasts prepareQC in pre-commit messages. After that, a replica responds to the Leader with pre-commit vote which has a signed digest of the proposal.

The commit step is similar to the pre-commit. What should be noted is that a replica becomes locked on the precommitQC at this time by setting its lockedQC to a precommitQC. This is of vital significance to insure the safety of the proposal in case it becomes a consensus decision.

What's more, the decide step means that when the Leader receives commit votes and combines them into a commitQC. Once the Leader has assembled one, it will send a commitQC in a decide message to all other replicas. Upon receiving a decide message, the replica considers the proposal saved in the commitQC and executes the commands in the committed branch. In the end, the replica increments viewNumber and starts the next view (see Fig.5).

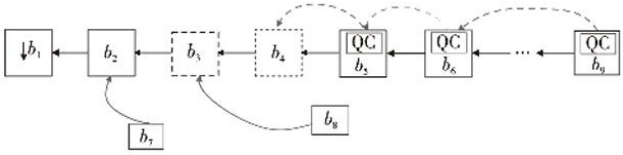

Fig. 5. HotStuff confirms the block process.

3.3 Diem

The most well-known practical application of HotStuff is Diem. Diem is the official name of Facebook's digital currency project. And its early name is Libra. As is announced by Facebook, Diem aims to provide cryptocurrency based on the US dollar

system. If this idea is successfully realized, Diem will surely be the first cryptocurrency to be issued by the big five technology company.

The Diem is a decentralized programmable database which is designed to support a low-volatility cryptocurrency. In the founders' vision, it would serve as an efficient medium of exchange for people of all classes all over the world. In the meantime, the founders present a proposal for the Diem protocol, which establishes the Diem blockchain and aims to make Diem a financial infrastructure where Financial services would be improved and innovated.

Unlike the permissionless blockchains, such as Bitcoin or Ethereum, the network of Diem only allows the highly vetted node operators to participate in, so it provides the basis for the regulatory compliance in this project.

Furthermore, there are two types of nodes on the Diem network structure: the Client and the Validator. The client can submit or query transactions, and the validator is responsible for processing those transactions and maintaining ledger updates in accordance with the Diem protocol. Besides, a set of replicas from different authorities, which is called validators, is designed to work together to maintain a database of programmable resources. In the meantime, transactions are based on predefined now. However, in future versions it will employ a new programming language called Move, which is going to change the smart contract to a user-defined version. As shown in Fig 6.

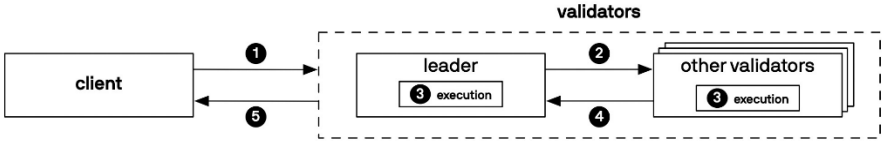

Fig. 6. Overview of the Diem protocol.

In addiction to what's talked about above, Diem uses the self-developed HotStuff consensus protocol instead of the traditional PBFT algorithm. Compared to the latter one, HotStuff improves the consensus efficiency and reduces latency, allowing Diem to process more transactions and maintain high throughput in the same time period.

3.4 Other Permissioned Blockchain Applications

To begin with, among the diverse application scenarios of blockchains, finance is considered to be the easiest to take the lead in landing and create the biggest actual value. Internationally, the blockchain-based J.P. Morgan Interbank Information Network (IIN) is expanding rapidly. As of September 2019, there has already been more than 330 banks, including the Deutsche Bank, expressing interest in joining it. And more than 65 of them have been officially launched in IIN since its launch in 2018. Besides, in China, as early as December 2017, China Merchants Bank succeeded in reaching a cooperation with Wing Lung Bank to realize the cross-border RMB remittance using blockchain technology between the three parties. Also, it has become the first inter-bank cross-border RMB liquidation business based on the blockchain technology all over the world.

In the second place, with the development of digital technology, the digital evidence appears more and more frequently in litigation cases. The unique characteristics of blockchain technology, such as non-tampering and decentralized storage, can solve the problem that the digital evidence is not easy to judge the authenticity and easy to disappear. At the same time, blockchain can reduce the cost of its storage and enhance the authenticity of digital evidence, thereby improving the efficiency of litigation.

Besides what's mentioned above, the government pays attentions to the application of blockchain in public services as well. As early as July 2017, Beijing issued a relevant work implementation plan, which clearly proposed to apply the blockchain technology to government services, indicating its approval of this emerging technology.

4 Challenges and Future

Nowadays, there are still some limitations to HyperLedger Fabric's architecture. First, its consensus mechanism can run into performance bottlenecks when processing a large number of transactions. Although its orderer nodes use Kafka to process transaction queues, the performance of Kafka could be affected in some high-concurrency scenarios. In addition, because HyperLedger Fabric's smart contracts are written in high-level languages such as Go, Node.js and Java, it may require high skill levels from the developers. At the same time, writing and debugging the chaincode also requires a certain amount of experience and skills.

To address these challenges, the HyperLedger Fabric community is constantly researching and innovating. For example, by trying to provide some more user-friendly development tools and platforms, the threshold for chaincode development is lowered, so that more developers can participate in the development of its applications.

When it comes to the HotStuff, its most prominent problem is that it relies heavily on the Leader. So as soon as a leader goes wrong, the whole algorithm is going to stop running.

About the Diem, it has been heavily criticized ever since it came to the public for the first time. At the time of the announcement, the project faced a number of regulatory hurdles, including the fact that the U.S. Senate and some European regulators did not support Facebook to issue a new digital currency. Since then, the Diem digital currency program has not developed as planned either. Although the project's designs are seemingly efficient and functional, it's still not completely different from the other blockchain projects. In addition, Diem's centralization issue may also lead to some internal divisions in the crypto community. And until now Facebook has not announced whether it will use Diem on its website, mobile app, and other affiliated products or not.

However, if all goes well, Diem will be the world's first cryptocurrency to be issued by the big technology company Facebook. On the top of that, Facebook, as a brand with global influence, is bound to be a huge help to Diem in terms of exchange listing and commercial adoption.

5 Conclusion

Initially seen as a tool to counteract banking and corporate dominance, blockchain technology has since transcended its roots to deliver widespread, universal benefits. As early as 2016, permissioned blockchains were gaining traction in specific sectors while permissionless chains, including a nascent Ethereum, were still under development, providing a fertile ground for permissioned variants to flourish. Technically, permissioned blockchains exhibit exceptional qualities, often surpassing other blockchain architectures in efficiency and security due to their controlled access mechanisms.

Despite their reduced level of decentralization—a trait that aligns with their commercial usage where some central control is necessary—permissioned blockchains have not seen a wane in corporate favor. Their adoption has escalated, with increasing recognition from businesses and governments of the cost efficiencies they offer. Consequently, these blockchains have carved out a significant niche in sectors where security, identity verification, and role definition are crucial. However, the primary challenges facing permissioned blockchains today are performance and scalability. The distinct consensus mechanisms and data storage techniques used in these systems differ fundamentally from traditional distributed databases, leading to potential bottlenecks in data processing and transaction speeds.

In conclusion, the evolution of blockchain technology is a clear, forward-moving trajectory. Yet, as it evolves, the ongoing integration and competition between permissioned and permissionless blockchains, alongside debates over their authenticity, are likely to remain central themes within the industry.

References

1. Sit, M. K., Bravo, M., & István, Z. (2021, June). An experimental framework for improving the performance of bft consensus for future permissioned blockchains. In Proceedings of the 15th ACM International Conference on Distributed and Event-based Systems (pp. 55-65).
2. Gupta, S., Hellings, J., Rahnama, S., & Sadoghi, M. (2020). Building high throughput permissioned blockchain fabrics: Challenges and opportunities. Proceedings of the VLDB Endowment, 13(12).
3. Zhu, X., Zhang, Y., Zhao, Z., & others. (2019). Radio frequency sensing based environmental monitoring technology. In Fourth International Workshop on Pattern Recognition (Vol. 11198, pp. 187-191). SPIE.
4. Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. arxiv preprint arxiv:2001.07091.
5. Amiri, M. J., Agrawal, D., & El Abbadi, A. (2021, June). Permissioned blockchains: Properties, techniques and applications. In Proceedings of the 2021 International Conference on Management of Data (pp. 2813-2820).
6. Lashkari, B., & Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. IEEE access, 9, 43620-43652.

7. Hao, Y., Li, Y., Dong, X., Fang, L., & Chen, P. (2018, June). Performance analysis of consensus algorithm in private blockchain. In 2018 IEEE Intelligent Vehicles Symposium (IV) (pp. 280-285). IEEE.
8. Ferdous, M. S., Chowdhury, M. J. M., & Hoque, M. A. (2021). A survey of consensus algorithms in public blockchain systems for crypto-currencies. Journal of Network and Computer Applications, 182, 103035.
9. Saha, A., & Sinha, B. B. An Exploration of Blockchain Technology: Applicability, Limitations, and Opportunities. In Intelligent Data Analytics, IoT, and Blockchain (pp. 240-251). Auerbach Publications.
10. Li, W., Feng, C., Zhang, L., Xu, H., Cao, B., & Imran, M. A. (2020). A scalable multi-layer PBFT consensus for blockchain. IEEE Transactions on Parallel and Distributed Systems, 32(5), 1146-1160.