Poster: A Weak Consensus Algorithm and Its Application to High-Performance Blockchain.

Qin Wang[2,4], Rujia Li[1,3], and Qi Wang[1]

[1] Southern University of Science and Technology, Shenzhen 518055, China.
[2] Swinburne University of Technology, Melbourne, VIC 3122, Australia
[3] University of Birmingham, Edgbaston, B15 2TT, Birmingham, United Kingdom
[4] HPB Foundation, DUO Tower, 189352, Singapore.
qinwang@swin.edu.au, rxl635@student.bham.ac.uk, wangqi@sustech.edu.cn

Abstract

A large number of consensus algorithms have been proposed. However, the requirement of strict consistency limits their wide adoption, especially in high-performance required systems. In this paper, we propose a weak consensus algorithm that only maintains the consistency of relative positions between the messages. We apply this consensus algorithm to construct a high-performance blockchain system, called *Sphinx*. We implement the system with 32k+ lines of code including all components like consensus/P2P/ledger/etc. The evaluations show that Sphinx can reach a peak throughput of 43k TPS (with 8 full nodes), which is significantly faster than current blockchain systems such as Ethereum given the same experimental environment. To the best of our knowledge, we present the first weak consensus algorithm with a fully implemented blockchain system.

MLA format

Qin Wang, Rujia Li. “A Weak Consensus Algorithm and Its Application to High-Performance Blockchain.” IEEE INFOCOM 2021-IEEE Conference on Computer Communications. IEEE, 2021.

BibTeX format

@inproceedings{wang2021a, title={A Weak Consensus Algorithm and Its Application to High-Performance Blockchain}, author={Wang, Qin and Li, Rujia}, booktitle={IEEE INFOCOM 2021-IEEE Conference on Computer Communications}, year={2021}, organization={IEEE} }

The links

The original link: https://infocom2021.ieee-infocom.org/accepted-paper-list-main-conference. The pre-print link: https://arxiv.org/pdf/2102.00872.pdf.

The paper has been accepted by INFOCOM 2021.

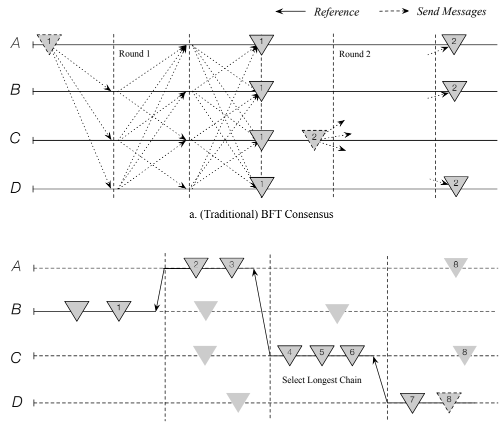
Poster: A Weak Consensus Algorithm and Its Application to High-Performance Blockchain

Qin Wang[2,4], **Rujia Li**[1,3], **Qi Wang**[1]

1.*Southern University of Science and Technology* 2.*Swinburne University of Technology*
3.*University of Birmingham* 4.*HPB Foundation*

Research Problem

Blockchain systems adopting the BFT consensus algorithm and Nakamoto consensus (NC) algorithm suffer from low-performance issues due to massive communication or intensive computation.



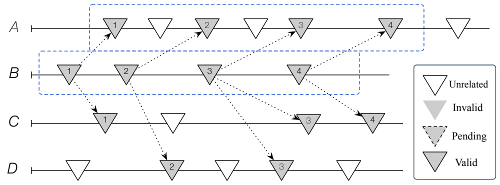
a. (Traditional) BFT Consensus

b. Nakamoto Consensus

Same principle. BFT-based and NC-based blockchain systems all require *strong consistency*, meaning that only one block is deemed as "valid" in different node in each round. This greatly constrains their overall performance since the procedures of conflict solving and total ordering are time-consuming.

Research Finding

We propose a new type of consensus mechanism, called *weak consensus*. Weak consensus guarantees that the relative sequences of blocks in one individual chain remain consistent with that in the other chains.



Example: The node B creates a serial of blocks $1, 2, 3, 4$. Our goal is to ensure that the relative order of $(B1 \to B2 \to B3 \to B4)$ is correctly maintained in nodes A, C and D. *(B1 represents the first block in node B.)*

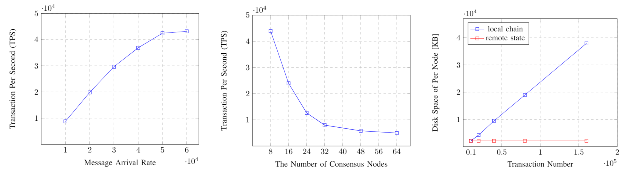
Detailed Algorithm

- ***Pre-prepare.*** The primary node receives the client requests and inserts the messages into local chain. Then, the node creates a *Pre-prepare* message to claim the relative position between two client messages.
- ***Prepare.*** A node receives the *Pre-prepare* message and checks the integrity, correctness, and validity. If the received *Pre-prepare* message passes the verification, the node updates his local-stored state and broadcasts the replied *Prepare* message to claim the correct relative position. Otherwise, the node aborts it.
- ***Commit.*** If any node receives a quorum $2f + 1$ of valid *Prepare* messages from peers within specified time interval, this node confirms the proposed decision by broadcasting a *Commit* message. When collecting more than $2f + 1$ *Commit* messages, the node transfers the state and replies to clients with updated state.

Complementary Mechanism. If a message (relative position) fails due to the lack of enough confirmation, the procedure of rebroadcast will be launched, and the counter increases each time of a retry. If the accumulated value is greater than the bound set in the counter, the node will accept the reversed relationship and rebroadcast it. If a node collects more than $2f+1$ *Commit* messages on the reversed position, the node replies to clients with updated state. Otherwise, the message will be aborted. On the other side, when the waiting time exceeds the predefined time-bound in the counter, the message will be aborted with sending a *timeout* message to the client.

System Evaluation

The average throughput of Sphinx reaches 43k TPS with 8 full nodes and drops to around 5000 TPS given 64 full nodes.



(a) TPS under Different Message Arrival Rates (b) TPS under Different Size of Nodes (c) Space Usage on Each Sphinx Node

- The throughput drops down as the number of participants increases.
- The throughput increases linearly (arrival rate <= 50k). The throughput flats out at around 43k TPS (arrival rate > 50k).
- The size of the local chain grows linearly with increased transactions.

Security Analysis

Relative persistence ensures that as soon as the relative position between two states has been confirmed by honest node, this relationship will ultimately be confirmed by every node in the network with a high probability.

Theorem 1. ***(Relative persistence)*** *If the relative position of two state y and x is accepted by the node N_i in iteration r and by the node N_j in $r+1$, respectively, their decisions on the relationship are the same.*

Liveness guarantees that all nodes eventually agree on a unique relationship *w.r.t* each chain.

Theorem 2. ***(Liveness)*** *If a correct relationship is committed in a honest node, then, every honest node will eventually accept such a relationship.*

Acknowledgements

Rujia Li and Qi Wang were supported by Guangdong Provincial Key Laboratory (Grant No. 2020B121201001). The authors would like to thank the team members from HPB foundation for their constructive suggestions.