SECURELY IMPROVING PERFORMANCE IN POW BLOCKCHAINS USING LINKS AND ANCHORS

OVIA SESHADRI

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
MAY 2023

SECURELY IMPROVING PERFORMANCE IN POW BLOCKCHAINS USING LINKS AND ANCHORS

by

OVIA SESHADRI
Department of Computer Science and Engineering

Submitted

in fulfillment of the requirements of the degree of

Doctor of Philosophy

to the

Indian Institute of Technology Delhi
May 2023

Certificate

This is to certify that the thesis titled **Securely Improving Performance in PoW Blockchains using Links and Anchors** being submitted by **Ovia Seshadri** for the award of **Doctor of Philosophy** in **Computer Science and Engineering** is a record of bona fide work carried out by her under my guidance and supervision at the Department of Computer Science and Engineering, Indian Institute of Technology Delhi. The work presented in this thesis has not been submitted elsewhere, either in part or full, for the award of any other degree or diploma.

Vinay Joseph Ribeiro
Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology Bombay
Powai, Mumbai - 400076

Subodh Vishnu Sharma
Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Delhi
Huaz Khas, New Delhi - 110016

Acknowledgements

First and foremost, I am honored to have Prof. Vinay J. Ribeiro. I thank him for his guidance, trust and patience during my vulnerable times. His knowledge inspired me and his humility grounded me. I also thank Prof. Subodh V. Sharma for his valuable inputs, support and supervision.

I thank all the faculty and staff of the Department of Computer Science and Engineering at IITD for their helping hand and providing the intellectual work space I needed. I am grateful to my lab mates and friends who have been like family to me the past seven years. They have aided in my research and molded my personality through many long and insightful discussions.

I thank my parents who dreamt of this long before I could dream of it. Their plans, sacrifices and encouragement gave me the skills and motivation I needed to endure this path. My mother, Rajeswari Seshadri, is the woman behind most of my achievements and this journey would not have been possible without her. I thank her for her effort, time and interest in the endless reviewing of my work and cheering me on till the end.

I am in debt to my loving husband, Karthick Sundaram, for his unequivocal support. He was proud of me in my highs and consoled me in my lows. He is the pillar of my strength and I am truly lucky to have him. I also thank my in-laws for their well wishes and prayers.

I thank all my teachers and mentors who have influenced and inspired me in small ways to lead me here today. Finally, I thank god for gifting me this life and the people in it.

Ovia Seshadri

Abstract

Proof-of-Work (PoW) blockchains add blocks, and consequently the chain weight, randomly. The blocks added also have a significant network delay owing to their large size. Large delay combined with randomness causes forks that are responsible for many security problems. One can reduce fork occurrences by designing a system with large block intervals and size but this design compromises performance aspects such as confirmation time guarantees. The trade-off between security and performance in PoW blockchain is a well discussed topic in the literature.

In this thesis, we aim to reduce the conflict between security and performance through our novel concepts of *Links* and *Anchors*. They are small, fast and frequent structures that can be incorporated on any new or existing PoW blockchains. They help reduce the confirmation time of its underlying blockchain while preserving its consistency security guarantees.

Our novel lower-bound chain growth rate for PoW systems with links or Anchors in the presence of a general adversary in a partially synchronous network, shows that they provide a more steady chain growth rate than classic PoW systems without them. On

a well-established, secure system like Bitcoin, we use the derived growth rate to show that when links or anchors are incorporated to Bitcoin, they help reduce its confirmation time from 60 minutes by half to 30 minutes, while retaining the consistency threshold guarantees of the original Bitcoin system. We provide a proof of concept emulation of links and anchors in a Bitcoin test bed consisting of 210 nodes having real world latencies between them. We benchmark a system with links and anchors against Bitcoin to show that they cause negligible network overheads and no compromises on security in terms of orphaned weight due to forks. Our theoretical analyses and experiments can easily be extended to other Nakamoto style PoW systems.

Title: लिंक और एंकर के उपयोग से पीओडब्ल्यू ब्लॉकचेन के सुरक्षित कार्य प्रणाली में सुधार लेना

Abstract in Hindi

प्रूफ़-ऑफ़-वर्क~(पीओडब्ल्यू) ब्लॉकचेन ब्लॉक जोड़ते हैं, और परिणामस्वरूप श्रृंखला का वजन, यादृच्छिक रूप से। जोड़े गए ब्लॉकों में उनके बड़े आकार के कारण महत्वपूर्ण नेटवर्क विलंब भी होता है।यादृच्छिकता के साथ संयुक्त बड़ी देरी फोर्क्स का कारण बनती है जो कई सुरक्षा समस्याओं के लिए जिम्मेदार हैं।बड़े ब्लॉक अंतराल और आकार के साथ एक सिस्टम को डिज़ाइन करके फोर्क की घटनाओं को कम किया जा सकता है लेकिन यह डिज़ाइन पुष्टिकरण समय की गारंटी जैसे प्रदर्शन पहलुओं से समझौता करता है। PoW ब्लॉकचेन में सुरक्षा और प्रदर्शन के बीच का समझौता साहित्य में एक अच्छी तरह से चर्चा का विषय है।

इस थीसिस में, हमारा लक्ष्य लिंक और एंकर की हमारी नई अवधारणाओं के माध्यम से सुरक्षा और प्रदर्शन के बीच संघर्ष को कम करना है। वे छोटी, तेज़ और लगातार संरचनाएं हैं जिन्हें किसी भी नए या मौजूदा पीओडब्ल्यू ब्लॉकचेन पर शामिल किया जा सकता है। वे इसकी स्थिरता सुरक्षा गारंटी को संरक्षित करते हुए इसके अंतर्निहित ब्लॉकचेन की पुष्टि के समय को कम करने में मदद करते हैं।

आंशिक रूप से सिंक्रोनस नेटवर्क में एक सामान्य प्रतिद्वंद्वी की उपस्थिति में लिंक या एंकर के साथ पीओडब्ल्यू सिस्टम के लिए हमारी नई निचली-सीमा श्रृंखला वृद्धि दर से पता चलता है कि वे उनके बिना क्लासिक पीओडब्ल्यू सिस्टम की तुलना में अधिक स्थिर श्रृंखला विकास दर प्रदान करते हैं।
बिटकॉइन जैसी अच्छी तरह से स्थापित, सुरक्षित प्रणाली पर, हम यह दिखाने के लिए व्युत्पन्न विकास दर का उपयोग करते हैं कि जब लिंक या एंकर को बिटकॉइन में शामिल किया जाता है, तो वे स्थिरता सीमा की गारंटी को बनाए रखते हुए इसके पुष्टिकरण समय को 60 मिनट से घटाकर आधा से 30 मिनट करने में मदद करते हैं। मूल बिटकॉइन प्रणाली का।

हम बिटकॉइन परीक्षण बिस्तर में लिंक और एंकर के अवधारणा अनुकरण का प्रमाण प्रदान करते हैं जिसमें 210 नोड्स होते हैं जिनके बीच वास्तविक दुनिया की विलंबता होती है। हम बिटकॉइन के खिलाफ लिंक और एंकर के साथ एक सिस्टम को बेंचमार्क करते हैं ताकि यह दिखाया जा सके कि वे नगण्य नेटवर्क ओवरहेड का कारण बनते हैं और फोर्क्स के कारण अनाथ वजन के मामले में सुरक्षा पर कोई समझौता नहीं करते हैं। हमारे सैद्धांतिक विश्लेषण और प्रयोगों को आसानी से अन्य नाकामोटो शैली पीओडब्ल्यू सिस्टम तक बढ़ाया जा सकता है।

Contents

List of Figures

List of Tables

List of Abbreviations

PoW	Proof of Work
HCR	Heaviest Chain Rule
LCR	Longest Chain Rule
BC	Blockchain
BTC	Bitcoin
ETH	Ethereum
CPU	Central Processing Unit
DS	Double Spend
SM	Selfish Mining
CT	Confirmation Time
RTF	Resolution Time of Fork
adv	adversary
hon	honest
SHA	Secure Hash Algorithm

P2P	peer to peer
RPC	Remote Procedure Call
JSON	JavaScript Object Notation
API	Application Prossessing Interface
VM	Virtual Machine
OS	Operating System
RAM	Random Access Memory
NTP	Network Time Protocol
MB	MegaByte
KB	KiloByte
GB	GigaByte
DAG	Directed Acyclic Graph
GHOST	Greedy Heaviest Object Sub-Tree
BFT	Byzantine Fault Tolerance
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof of Stake
PoR	Proof of Resource
PoST	Proof of Space Time
PoA	Proof of Authority