

SECURELY IMPROVING PERFORMANCE IN POW BLOCKCHAINS USING LINKS AND ANCHORS

OVIA SESHADRI



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI

MAY 2023

© Indian Institute of Technology Delhi (IITD), New Delhi, 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

प्रूफ-ऑफ-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 नाकामोटी शैली पीओडब्ल्यू सिस्टम तक बढ़ाया जा सकता है।

Contents

Certificate	i
Acknowledgements	iii
Abstract	v
List of Figures	xv
List of Tables	xxi
List of Acronyms	xxii
1 Introduction	1
1.1 Background	2
1.2 Motivation	6
1.3 Research Goals	8

1.4	Contributions	9
1.5	Organization of the Thesis	10
2	Literature Review	15
2.1	Reducing Block Size and Interval	15
2.2	Altering the Linear Blockchain Structure	16
2.3	Using Weak Blocks	18
3	Links	21
3.1	Structure	22
3.2	Determining Chain Weight with Links	22
3.3	Link Generation and Processing	24
3.4	Delay Model	26
3.5	Fork Resolution	27
3.6	Link Rewards	28
4	Theoretical Evaluation of Links	29
4.1	System and Adversary Model with Links	29
4.2	Chain Growth For Links	31
4.3	Confirmation Time with Links	38
4.3.1	Double spend attack in a system with links	38

4.3.2	Apriori CT analysis for links	39
4.3.3	Time variant CT in links	44
4.4	Selfish Mining	49
4.4.1	Attacker's strategy	50
4.4.2	Markov chain	55
4.4.3	Stationary probabilities	55
4.4.4	Revenue	56
4.4.5	Observations on the selfish mining analysis	59
4.5	Chain Quality with Links	60
4.6	Consistency with Links	61
4.6.1	Preliminaries	63
4.6.2	Blocktree partitioning of a blockchain with links	64
4.6.3	Nakamoto entity for a system with links	66
4.6.4	Observations on consistency with links	68
4.6.5	Note on Systems that Reduce Block Sizes and Interval	69
4.7	Conclusion of the Theoretical Evaluation on Links	70
5	Experimental Evaluation of Links	71
5.1	Modifications Made to Bitcoin	71

5.2	Network Overlay Structure	73
5.3	Experiments on Propagation Delay	73
5.3.1	Propagation delay vs block sizes	75
5.3.2	Effect of block delay with and without links	76
5.4	Forks and Orphaned Weight	77
5.4.1	Varying block size and interval at a fixed throughput	78
5.4.2	Classic blockchain vs links and fork prevention	78
5.4.3	Resolution Time of Forks (RTF)	79
5.5	Conclusion of the Experimental Evaluation on Links	81
6	Anchors	83
6.1	Structure	84
6.2	Anchor Mining	85
6.3	Determining Chain Weight with Anchors	86
6.4	Anchor Processing	87
6.5	Delay Model	89
6.6	Fork Resolution with Anchors	89
6.7	Rewarding Anchors	90
6.8	Note on the Analyses between Links and Anchors	91

7	Theoretical Evaluation of Anchors	93
7.1	System and Adversary Model with Anchors	93
7.2	Chain Growth with Anchors	95
7.3	Confirmation Time with Anchors	102
7.3.1	Double spend attack in a system with anchors	103
7.3.2	Apriori CT analysis for anchors	104
7.3.3	Observations on the apriori analysis	113
7.3.4	Time variant CT in anchors	114
7.4	Chain Quality with Anchors	125
7.5	Consistency with Anchors	126
7.5.1	Preliminaries	129
7.5.2	Blocktree partitioning of a blockchain with anchors	130
7.5.3	Nakamoto block for a system with anchors	132
7.5.4	Observations on consistency with anchors	133
7.6	Forking Analysis	134
7.6.1	Fork resolution with honest miners	135
7.6.2	Fork resolution analysis	135
7.6.3	Prolonged fork attack	139
7.7	Anchor Rewards	140

7.7.1	Delayed anchor broadcast attack	142
7.7.2	Anchor rewards analysis	143
7.8	Conclusion of the theoretical evaluation on anchors	146
8	Experimental Evaluation of Anchors	147
8.1	Modifications made to Bitcoin	147
8.2	Network Overlay Structure	149
8.3	Experiments on Propagation Delay	149
8.4	Resolution Time of Forks (RTF)	152
8.5	Fork Prevention	153
8.6	Conclusion of the Experimental Evaluation on Anchors	155
9	Comparison of Links and Anchors	157
9.1	Structure	157
9.2	Generation and Processing	158
9.3	Forks	158
9.4	Chain Weight	159
9.5	Chain Growth	159
9.6	Rewards	160
9.7	Adversary Attacks	160

9.8 Combining Links and Anchors	162
10 Conclusion and Future Scope	165
10.1 Summary of the Thesis	165
10.2 Future Research Directions	168
Appendices	169
A Other Methods of Evaluating Consistency	171
A.1 Consistency with Links	173
A.1.1 Convergence Opportunities (CO) with Links	174
A.1.2 Breaking Convergence	175
A.1.3 Note on Systems that Reduce Block Sizes and Interval	177
A.2 Consistency with Anchors	179
A.2.1 Convergence Opportunity (CO) with Anchors	179
A.2.2 Breaking Convergence	180
A.2.3 Stationary and Transitional probabilities for CO	181
A.2.4 Analysis	189
A.2.5 Consistency	192
B Latencies between world cities	195

Bibliography	201
List of Publications	207
List of Patents	209
Biography	211

List of Figures

1.1	Sample blockchain	2
1.2	Sample Block Contents	3
1.3	Target space division	3
1.4	Sample fork in a blockchain system	4
3.1	Sample blockchain with links	22
3.2	Link Contents	23
3.3	Target division with links	23
4.1	Marking process towards chain growth for Links	34
4.2	CT comparison at link frequency $l = 2$ at various block confirmations (k) of systems with and without links	43
4.3	$q = 28\%$ and $l = 5$	48
4.4	$l = 5$	49

4.5	$q = 28\%$	50
4.6	State machine with transition frequencies	54
4.7	Effects of q and γ for a selfish mining attack on a system with links compared to original results from [1]	59
4.8	Loner block in a system with links	66
4.9	Loner link in a system with links	66
4.10	Maximum adversary tolerance at various block intervals between classic PoW systems and system with links	69
5.1	Sample illustration of the network setup phase with links.	74
5.2	Propagation delay of various block sizes	75
5.3	Delay of $\approx 1\text{MB}$ blocks with and without the presence of links	76
5.4	Orphaned weight over classic PoW blockchains with varied blocks (size, intervals) at a fixed transaction throughput	78
5.5	Orphaned weight between classic PoW system, system with links	79
5.6	Sample scenario depicting faster fork resolution with links	80
5.7	Mean resolution time of forks in system without links ($l=0$) and with links ($l=2,5,10$)	81
6.1	Sample blockchain with anchors	84
6.2	Anchor Contents	85

6.3	Target division with anchors	85
7.1	Marking process towards chain growth with anchors	98
7.2	CT comparison at $a = 2$	112
7.3	Apriori success vs q at $a = 2, 5$ and $k = 6$, comparison of results from [2](without anchors) and anchors	114
7.4	Apriori success vs q comparison of result from [2](without anchors) and this work at $a = 2$ for various k	115
7.5	Sample scenario for the time variant double spend analysis. Timeline of arrival of Blocks and Anchors on the attacker node	116
7.6	Chance of a Double Spend Attack with and without Anchors where the attacker owns $q = 17\%$ of the network hashpower. Anchors are generated at $a = 5$ Anchors/block	123
7.7	Chance of a Double Spend Attack with and without Anchors varying attacker hashpower and Anchors are generated at $a = 5$ Anchors/block	123
7.8	Varying Anchor frequency with 17% attacker hash power	124
7.9	Loner block in a system with anchors	131
7.10	Adversary tolerance at various block intervals between classic PoW systems and system with anchors	134
7.11	System forked into two branches splitting the honest hashing power as p_1 and p_2 between Branch 1 and 2 respectively where $p_1 + p_2 = 1$	136

7.12	Timeline of arrivals as seen on a mining peer on the network in the worst case. The time at which a valid fork is recognized is t . The miner has accepted Block B_k^1 before seeing Block B_k^2 . The anchor resolving this fork is seen by the miner at $t + T$	136
7.13	Strategies of the Quasi-Honest Miner to maximize anchor rewards	144
8.1	Sample illustration of the network setup phase with anchors.	150
8.2	Delay of $\approx 1\text{MB}$ blocks with and without the presence of anchors	151
8.3	Sample scenario depicting faster fork resolution with anchors	153
8.4	Mean fork resolution time with 95% confidence intervals	154
8.5	Sample scenario depicting fork prevention with anchors	154
8.6	Mean number of forks prevented with 95% confidence intervals	155
9.1	Illustrative depiction of the target space division in a system having both anchors and links	162
9.2	Illustrative depiction of a system having both anchors and links	163
A.1	Convergence opportunity in classic PoW blockchains	172
A.2	Convergence Opportunities in a system with links (a) Type-1 convergence of an honest link and (b) Type-2 convergence of an honest block.	175
A.3	Maximum adversary tolerance threshold at various block intervals as per Theorem A.1.4	178

A.4	At a fixed q , we find the ratios of the permitted block interval (c) using links over the c permitted by Kiffer et.al. [3].	178
A.5	Convergence Opportunities in a system with anchors (a) Type-1 convergence of an honest anchor and (b) Type-2 convergence of an honest block.	180
A.6	Markov model for counting COs	181
A.7	Maximum adversary tolerance threshold at various block intervals as per Theorem A.2.4 compared with [4, 3].	194
A.8	At a fixed q , we find the ratios of the permitted block interval (c) using anchors over the c permitted by Kiffer et.al. [3].	194

List of Tables

1.1	Comparison of links and anchors	11
1.2	A high-level view of the chapters and contents in this thesis	12
4.1	Summary of variables introduced for the theoretical analyses on links . . .	31
7.1	Summary of variables introduced for the theoretical analyses on anchors . .	95
9.1	Comparison of links and anchors	161
B.1	Latencies between world cities in milliseconds [5] table 1 out of 4	196
B.2	Latencies between world cities in milliseconds [5] table 2 out of 4	197
B.3	Latencies between world cities in milliseconds [5] table 3 out of 4	198
B.4	Latencies between world cities in milliseconds [5] table 4 out of 4	199

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