

Fair and Regulated Resource Allocation in Blockchain based Decentralized Systems

ADITYA AHUJA



Department of Computer Science and Engineering
Indian Institute of Technology Delhi
May 2022

©Indian Institute of Technology Delhi
2022
All rights reserved.

Dedicated to:
The Light within All Beings,
and my Parents.

Fair and Regulated Resource Allocation in Blockchain based Decentralized Systems

by

ADITYA AHUJA

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 2022

Certificate

This is to certify that the dissertation titled *Fair and Regulated Resource Allocation in Blockchain based Decentralized Systems*, submitted by MR. ADITYA AHUJA for the award of *Doctor of Philosophy in Computer Science and Engineering*, is a record of bona fide work carried out by him under our 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 J. Ribeiro

Associate Professor

Department of Computer Science and Engineering

Indian Institute of Technology Bombay

Powai, Mumbai - 400076



Subodh V. Sharma

Assistant Professor

Department of Computer Science and Engineering

Indian Institute of Technology Delhi

New Delhi - 110016

Acknowledgements

First and foremost, I would really like to thank my advisor, Prof. Vinay J. Ribeiro (Associate Professor, IIT Bombay), for his unwavering trust in my abilities and his support, and for entertaining my personal research ambitions. Vinay sir has been a witness to my entire journey, and has stuck with me through thick and thin. Although I should concede that I was not fully receptive to his inputs over the years, I now realize in hindsight that his constructive criticism was correct, and has forged me into what I am today. I would like to thank Prof. Subodh V. Sharma (Assistant Professor, IITD) for his oversight. I would like to thank Dr. Rajeev Shorey (adjunct faculty, IIT Delhi) for hosting me at the TCS Innovation Labs, where with him I discovered the integrity and merit behind the pursuit of academic research. Rajeev sir is an eternal optimist, and would always lend a kind ear to any problem I faced (which he could address). I would like to thank Prof. Leana Golubchik (Professor, USC) for hosting me in her distributed systems group at USC. Leana ma'am's polite and simple, yet profound interventions, helped me greatly to develop my work, and improve the way it is presented to the public. Finally, and to a great extent, I would like to thank Dr. Ranjan Pal (faculty member, UMich Ann Arbor), who over the years has helped me in refining my ability and skills in idea formation and scientific writing. Ranjan sir helped me on my idea communication ability over an extended period of time, and was incredibly supportive. I was fortunate enough to work with him on some other stability and efficiency (economics related) problems in distributed systems, during my time at USC and beyond.

Apart from this, I would like to thank my colleagues (especially Himanshu Gandhi among them) in the doctoral programme in the systems security group at the CSE and SIT departments, for their supportive nature over the years. I would also like to thank the administrative staff of the CSE and SIT departments for lending a helpful hand whenever needed.

Aditya Ahuja

Abstract

With the birth and gradual prevalence of the Internet, conventional wisdom dictated the development and use of centralized computational systems: systems that enabled services suffering from the problem of being a central point of trust, and also a single point of failure. With the proposal of the first blockchain based decentralized, crypto-economic service in the form of Bitcoin (circa 2009), there has been a revival of interest in the principle of defining *systems with decentralized autonomy*: building peer-to-peer services without a central point of trust, or even trust in the peers of the network. Instead, the trust resides in the protocol that defines the decentralized system and the associated application. Given this general principle, there has been an explosion in the number of blockchain consensus based decentralized services around the globe, spanning the sectors of finance, government, healthcare, and logistics (among others). However, till date, the most prominent use case of blockchains has been in defining decentralized financial applications, and more narrowly in serving as a foundation for cryptocurrencies.

In this dissertation, we first propose a decentralized lottery that is amenable to be deployed on a cryptocurrency network. Decentralized lotteries require access to high speed and high quality distributed randomness, for fairly choosing lottery winners. Classically, achieving high speed deterministic randomness in the presence of an adversary is non-trivial. Fortunately, revisiting the age-old binary agreement (Byzantine agreement) problem through a quantum protocol provides a solution towards this requirement. We leverage both blockchain consensus and quantum binary agreement to develop a theoretical decentralized lottery solution.

Another problem of interest to the distributed systems community (and in no small measure to the regulatory bodies around the world) is the proposal and confirmation of legal transactions as part of the blockchain consensus of prominent cryptocurrencies. It is necessary that all cryptocurrency transactions be consistent with the legal rules of the federal jurisdiction within which they have been proposed. Thus, financial regulators of various federal governments must

have a say in the structure and validity of cryptocurrency transactions. As a second contribution, we provide a consensus based regulatory framework and a theoretical system to maximize the throughput of legal transactions in cryptocurrency blockchains. Our method is a stark departure from previous regulatory policies, as it maximizes the legal transaction throughput as a function of the total regulated consensus resource in the blockchain system.

सार:

इंटरनेट के जन्म और अधिक प्रसार के साथ, पारंपरिक ज्ञान ने कैम्प्यूटरीकरण सिस्टम के विकास और उपयोग को निर्धारित किया: जिस ज्ञान के केंद्रीय बिंदु होने की संख्या से पीछे सेवाओं को सक्षम करता है, और विचारता का एक बिंदु भी। डिजिटल (जून 2009) के रूप में पहली पारंपरिक आधारित विकेन्ट्रीकृत, डिप्टो-अर्थिक सेवा के प्रसार के साथ, विकेन्ट्रीकृत व्यवसाय ने साथ सिस्टम को परिभाषित करने के सिद्धांत में रुचि का पुनर्ग्रहण हुआ है। पौरुष-दु-पौर सेवाओं का निर्माण सिस्टम का केंद्रीय बिंदु, या नेटवर्क के सभियों में भी भरोसा। इस कारण, टाट उस प्रोटोकॉल में रहता है जो विकेन्ट्रीकृत प्रणाली और संबंधित अनुप्रयोग से परिभाषित करता है। इस कारण सिद्धांत को देखते हुए, दुनिया भर में पारंपरिक संरचनात्मक आधारित विकेन्ट्रीकृत सेवाओं की संख्या में विलम्ब हुआ है, जो फिर, सरकार, साम्य सेवा और रक्त (अप के बीच) के क्षेत्रों में फैले हुए हैं। हालांकि, आज तक, पारंपरिक का सबसे प्रमुख उपयोग विकेन्ट्रीकृत वित्तीय अनुप्रयोगों को परिभाषित करने में रहा है, और डिप्टोकॉली के लिए एक पीर के रूप में सेवा करने में अधिक संश्लेषण है।

इस बीच प्रबंध में, हम पहले एक विकेन्ट्रीकृत लॉटी का प्रसार करने हैं जिसे एक डिप्टोकॉली नेटवर्क का लेना किया जा सकता है। विकेन्ट्रीकृत लॉटी को लॉटी विचारों को उचित रूप से चुनने के लिए उच्च गति और उच्च पुनरावृत्ति विनिर्दिष्टता तक पहुंच की आवश्यकता होती है। साम्य रूप से, एक विशेषी की उपस्थिति में उच्च गति निष्पादनक वास्तुशिक्षा प्राप्त करता है। कुछ है। लौ-रूप से, सर्वोच्च प्रोटोकॉल के माध्यम से सभियों चुनने बाइनी एसेमेंट (बी-सभियन एसेमेंट) संख्या को फिर से देखना इस आवश्यकता के लिए एक संस्थापन प्रदान करता है। सैद्धांतिक विकेन्ट्रीकृत लॉटी संस्थापन विकसित करने के लिए हम पारंपरिक संरचनात्मक और सर्वोच्च बाइनी सभियों टोनों का साथ उठाते हैं।

विनिर्दिष्ट सिस्टम अनुदाय के लिए ध्यान की एक और संख्या (और दुनिया भर के निष्पादन विचारों के लिए कोई छोटा उदाहरण नहीं है) प्रमुख डिप्टोकॉली के पारंपरिक संरचनात्मक के दिग्गो के रूप में कानूनी लेनदेन का प्रसार और पुष्टि है। यह आवश्यक है कि सभी डिप्टोकॉली लेनदेन संघीय क्षेत्रविकास के कानूनी विचारों के अनुसार हैं, जिसके पीछे उन्हें प्रसारित किया गया है। इस प्रकार, विभिन्न संघीय सरकारों के वित्तीय विचारों को डिप्टोकॉली लेनदेन की संख्या और फैला में एक कदम बढ़िए। दूसरे संस्थापन के रूप में, हम डिप्टोकॉली पारंपरिक में कानूनी लेनदेन के सुदूर को अधिकृत करने के लिए एक आम सभियन आधारित निष्पादनक संस्था और एक सैद्धांतिक प्रणाली प्रदान करते हैं। हमारा लक्ष्य विश्वी निष्पादनक लॉटी में किन्तुल आना है, क्योंकि यह पारंपरिक सिस्टम में कुछ विनिर्दिष्ट आम सभियन संस्थापन के एक कार्य के रूप में कानूनी लेनदेन सुदूर को अधिकृत करता है।

Contents

Certificate	i
Acknowledgements	iii
Abstract	v
List of Figures	xiv
List of Acronyms	xvii
1 Introduction	1
1.1 Preliminaries: Distributed Consensus and Blockchains	1
1.1.1 Background on Blockchain Consensus	1
1.1.2 Network Membership and Proof-of-Resource Blockchains	2
1.1.3 The Network Model	3
1.1.4 The Adversary Model	3
1.2 The Problem Setting	4
1.2.1 Decentralized Lotteries for Cryptocurrency Networks	4
1.2.2 Blockchain based Regulated Decentralized Crypto-Economies	4
1.3 Our Contributions	5

1.3.1	Scope of our Contributions: A Qualitative Analysis of the Proposed Decentralized Systems	7
2	Fundamentals of Distributed Consensus	9
2.1	The General Principles for Distributed Consensus	9
2.1.1	Modelling the Network for Consensus	9
2.1.2	The Definition of Distributed Consensus	10
2.1.3	The Adversary Model for corrupting Consensus	11
2.1.4	Performance Measures for Consensus Protocols	12
2.2	Binary Agreement: Byzantine Broadcast and Byzantine Agreement	12
2.3	Blockchain Consensus	13
2.3.1	Other Blockchain Protocol Properties	14
2.3.2	Network Membership Model and the Consensus Resource	15
2.3.3	The Adversary Model	15
2.3.4	(Economic) Incentivization in Blockchains	16
2.3.5	Blockchains for Cryptocurrencies	16
2.4	State Machine Replication	16
2.5	Quantum Binary Agreement	17
2.5.1	BFT Quantum Binary Agreement	17
2.5.2	A Practical Realization	19
3	A Study on Sourcing Distributed Randomness	21
3.1	The Need for Randomness Beacons	21
3.2	Classical BA Protocols are Slow (Per Bit)	22
3.3	SMR Protocols are Slow in the Worst Case	22

3.4	Randomness through the Blockchain State or Protocol	23
3.5	Other Distributed Randomness Beacon Protocols	24
3.6	Quantum BA gives Fast Deterministic Randomness	25
4	TensorFlip: A Fair and Fast Decentralized Lottery	27
4.1	Defining a Novel Decentralized Lottery	28
4.1.1	Traditional Centralized Lotteries	29
4.1.2	The TensorFlip Decentralized Lottery System	29
4.1.3	The Definition of Lottery Consensus	30
4.2	The Execution Model	31
4.2.1	The Network (Communication) Model	31
4.2.2	The Threat (Fault) Model	31
4.3	Preliminary Definitions and Constructions	32
4.3.1	Full Decentralization	32
4.3.2	Basics of Quantum Computing as relevant to Consensus	32
4.3.3	Basics of Cryptographic Sortition	33
4.4	An Overview of TensorFlip	33
4.4.1	Notation	33
4.4.2	Outline of the Lottery Agreement	34
4.4.3	Token Transfer and Computation of User Winnings	36
4.5	Crash-Fault Tolerant TensorFlip Protocol	38
4.5.1	The Fail-Stop TensorFlip Distributed Algorithm	38
4.5.2	Features of Fail-Stop TensorFlip	38
4.6	Byzantine-Fault Tolerant TensorFlip Protocol	40

4.6.1	The Byzantine TensorFlip Distributed Algorithm	40
4.6.2	A Brief Security Analysis	41
4.6.3	Features of Byzantine TensorFlip	42
4.7	TensorFlip on an Asynchronous Network	44
4.7.1	Limitations of Classical Consensus	44
4.7.2	Leveraging Blockchain and Quantum Consensus in the Asynchronous Setting	45
4.7.3	A Stepping Stone to a Fully Quantum Protocol	45
4.8	Generalizing TensorFlip: Blockchain Nodes separate from Lottery Players . . .	45
4.9	Quantum Advantage: Expected Constant Round Complexity with Deterministic Randomness	46
4.10	Comparison with Existing Lotteries	46
5	A Survey on the Status of Regulation of Cryptocurrency Blockchains	49
5.1	Motivating Regulation with a Study of the Silk Road Market	49
5.1.1	Illicit Transactions employing Bitcoin	50
5.2	Need for Regulated Blockchains and Regulatory Policy Status	51
5.2.1	Features necessary in a Blockchain for Regulated Trade	52
5.2.2	Limitations of existing Blockchains in achieving all Features of Regulated Trade	53
5.2.3	Existing State of Cryptocurrencies and Regulatory Policymaking	54
5.3	On-Chain Regulatory Enforcement: Motivation for a Regulated Blockchain Protocol	55
6	A Regulatory System for Maximizing the Legal Transaction Throughput	59
6.1	A System Model for Regulated Blockchains	62

6.1.1	A Brief on Blockchain Consensus	62
6.1.2	Stakeholders, Terminology, Assumptions, and Notation	63
6.1.3	Regulated Blockchain System Design Goals	66
6.1.4	Regulated Blockchain Protocol Features	67
6.1.5	Block Proposal Competition between Regulated and Unregulated Ex- ecutors	68
6.2	Regulated Blockchain Protocols	70
6.2.1	Regulated Blockchain Consensus for Bitcoin	70
6.2.2	Regulating Nxt Proof-of-Stake	72
6.2.3	Competition in a Regulated Setting	72
6.3	Competition Analysis for Maximizing Legal Transaction Throughput	73
6.3.1	The Regulated Blockchain Game Features	73
6.3.2	A Stochastic Game with Immediate Block Release	77
6.3.3	A Stochastic Game with Immediate Block Release and an Oversight Compliance Fee	79
6.3.4	A Stochastic Game with Strategic Block Release by Regulated Executors	82
6.3.5	The Consensus Resource Thresholds	84
6.3.6	Tying the Results with Existing Protocols	84
6.3.7	Discussion: Practical Application to Bitcoin	85
6.3.8	The General Implication of our Results	87
6.4	Outline: Regulated Executors Stalling an Illegal Blockchain	87
6.5	Proofs of the Competition Analysis Theorems	89
6.5.1	Regulated Blockchain Stochastic Games	89
6.5.2	Proof of Theorem 5	90

6.5.3	Proof of Theorem 6	91
6.5.4	Proof of Theorem 7	91
7	Summary and Future Directions	95
7.1	TensorFlip: Practicality and Alternate Applications	95
7.2	Regulatory System: Alternate Analysis and Oversight Policy	96
7.3	Discussion: Coexistence of our Solutions	97
Appendices		
Appendix A	Solutions towards Network Security	101
A.1	PlumeWalk: A Threat Provenance Analytic Framework	101
A.1.1	Contribution Summary	102
A.2	SpectraMap: A Spatio-Temporal RF Spectrum Occupancy Map	104
A.2.1	Contribution Summary	105
A.2.2	The Need for RF Spectrum Maps and the Utility of SpectraMap	107
Bibliography		111
8	List of Publications	123
8.1	Published Papers	123
8.2	Preprints	124
Biography		127

List of Figures

1.1	A stack-level view of our contributions towards contemporary decentralized systems. The two consensus layer contributions imply two decentralized applications at the application layer. We also give two additional contributions (in the Appendix) towards network security.	6
4.1	TensorFlip is technically more viable than permissionless blockchains, and classical consensus protocols for defining a decentralized lottery, given a synchronous network with fail-stop or Byzantine adversaries. Permissionless blockchains can never be fully decentralized [KLK ⁺ 19], and classical BA protocols are slow [BOH05]. Also, SMR protocols need re-engineering to formally ensure full-decentralization.	28
4.2	Summary of symbols used in the TensorFlip protocols.	34
4.3	Step-by-step overview of the TensorFlip lottery protocol with 5 lottery users, under a Byzantine adversary. (1) Each user $i \in \{1, 2, \dots, 5\}$ gossips the lottery parameters $(\pi_i^{\text{bet}}, \pi_{i,0}^{\text{house}}, \pi_{i,1}^{\text{house}})$ (bet and house messages) over the classical network. (2) The lottery users agree on the lottery parameters for all users, using blockchain consensus over the same classical network. (3) The users run a quantum BA consensus protocol to elect the house (user 4 elected as per the depiction), over a quantum network. (4) Each user locally computes the winnings for all users, using the bet message confirmed per user from step (2), house odds message by user 4 confirmed in step (2), and the HashBin routine.	37
6.1	Traditional vs Regulated Blockchain Systems	62
6.2	Notation for our Regulatory Framework	65

6.3	Toy Model of a Permissionless Regulated Blockchain Network. Regulatory body (center) licenses four executors $\{2, 5, 6, 9\}$ (highlighted with a regulatory stamp on the associated coin miner) to propose regulated blocks. The remaining executors are free to propose any type of blocks.	69
6.4	A summary of the results of our regulatory system. When $\alpha_R \leq h_{IR}^{ocf}$, the legal transaction throughput $t_{\mathcal{F}}$ can be unfairly increased only when $\alpha_R \geq \hat{h}_{SR}$, under the longest branch rule (gray curve indicates dubious blocks). However, when $\alpha_R > h_{IR}^{ocf}$, the longest legal branch rule wins (blue curves indicating legal blocks), unregulated executors can do no better than proposing legal blocks, and the legal transaction throughput is maximized. When $h_{IR}^{ocf} < \alpha_R < h_{IR}$, the regulator needs to invest a compliance fee $\rho_{\mathcal{F}}$ in the regulated blocks. Consensus thresholds h_{IR} , h_{IR}^{ocf} , and \hat{h}_{SR} are defined later.	75
6.5	When $\geq 58\%$ of the consensus resource in the blockchain network is regulated, the legal branch (right) corresponding to the regulated executors R wins, by forcing \bar{R} to abandon and defect from their branch. Note that regulated blocks are denoted by \mathbb{RB} , legal blocks are denoted by \mathbb{LB} , and dubious blocks are denoted by \mathbb{DB} . The root block is denoted by \mathbb{B}^0	78
6.6	Upperbound on the Unregulated Consensus Resource for the RegFrontier/LegFrontier strategies, as a function of the Game Depth (base results from [KKKT16]).	79
6.7	When $> 50\%$ of the consensus resource in the blockchain network is regulated, and the regulator adds an OCF (denoted by the money bag in the \mathbb{RB} blocks), the legal branch (right) corresponding to the regulated executors R wins, by forcing \bar{R} to abandon and defect from their branch.	81
6.8	When $> 33\%$ but less than a majority of the consensus resource in the blockchain network is regulated, the regulated executors R can force the unregulated executors \bar{R} to abandon and defect from their branch through strategic release (unreleased \mathbb{RB} block denoted by a dashed box in epoch $e_0 + 4$).	83
A.1	PhameWalk can capture cross tier attack interpretations: A malicious operator compromises device data to mistrain the enterprise machine-learning classifier in an Industrial IoT network.	104
A.2	Toy view of SpectraMap: The deployment of static and mobile sensors to build a space-time RF map	107

List of Acronyms

ABC	<i>Asynchronous Blockchain without Consensus</i>
BA	<i>Byzantine Agreement</i>
BB	<i>Byzantine Broadcast</i>
BDoS	<i>Blockchain Denial of Service</i>
BFT	<i>Byzantine Fault Tolerant</i>
CBDC	<i>Central Bank Digital Currency</i>
CPS	<i>Cyber Physical Systems</i>
CRHF	<i>Collision Resistant Hash Function</i>
CVE	<i>Common Vulnerability and Exposure</i>
DNS	<i>Domain Name System</i>
FCC	<i>Federal Communications Commission</i>
GST	<i>Global Stabilization Time</i>
IIoT	<i>Industrial Internet of Things</i>
IoT	<i>Internet of Things</i>
IoV	<i>Internet of Vulnerabilities</i>
IR	<i>Immediate (Block) Release</i>
KYC	<i>Know Your Customer</i>
MDP	<i>Markov Decision Process</i>
MICA	<i>Markets in Crypto Assets</i>
NTIA	<i>National Telecommunications and Information Administration</i>
NTP	<i>Network Time Protocol</i>
OCF	<i>Oversight Compliance Fee</i>
OWASP	<i>Open Web Application Security Project</i>
PBFT	<i>Practical Byzantine Fault Tolerance</i>
PGP	<i>Pretty Good Privacy</i>
PoR	<i>Proof of Resource</i>
PoS	<i>Proof of Stake</i>

PoW	Proof of Work
QBA	Quantum Byzantine Agreement
QVSS	Quantum Verifiable Secret Sharing
REM	Radio Environmental Map
RO	Random Oracle
RSSI	Received Signal Strength Indicator
SM1	The First Selfish Mining Attack (Bitcoin)
SMR	State Machine Replication
SR	Strategic (Block) Release
UAV	Unmanned Aerial Vehicle
VRF	Verifiable Random Function