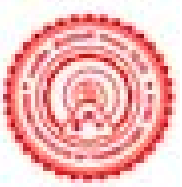
Fair and Regulated Resource Allocation in Blockchain based Decentralized Systems

ADITYA AHUJA



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

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

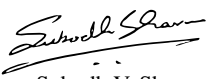
Indian Institute of Technology Delhi

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 आर्थिक प्रसार के साथ, पारंपरिक इस्त ने केंद्रीकृत कम्प्यूटेशनल सिस्टम के विकास और उपयोग को निर्धारित किया: सिस्टम जो विकास के केंद्रीय बिंदु होने की समस्या से पीड़ित सेवाओं को सहज बनाता है, और विफलता का एक बिंदु भी। बिटकॉइन (सतोशी 2009) के रूप में पहली ब्लॉकचेन आधारित विकेन्द्रीकृत, क्रिप्टो-आर्थिक सेवा के प्रसार के साथ, विकेंद्रीकृत व्यवस्थाओं के साथ सिस्टम को परिभाषित करने के सिद्धांत में रुचि का पुनरुद्धार हुआ है: पीयर-टू-पीयर सेवाओं का नियोजित विकास का केंद्रीय बिंदु, या नेटवर्क के सामियों में भी भागीदार। इसके बावजूद, ट्रस्ट उन प्रोटोकॉल में रहता है जो विकेंद्रीकृत प्रणालियों और संबंधित अनुप्रयोग का परिभाषित करता है। इस सामान्य सिद्धांत को देखते हुए, दुनिया भर में ब्लॉकचेन सार्वजनिकी आधारित विकेन्द्रीकृत सेवाओं की संख्या में विस्फोट हुआ है, जो वित्त, सरकार, सामान्य सेवा और रसद (अन्य के बीच) के क्षेत्रों में फैले हुए हैं। हालाँकि, आज तक, ब्लॉकचेन का सबसे प्रमुख उपयोग विकेंद्रीकृत वित्तीय अनुप्रयोगों को परिभाषित करने में रहा है, और क्रिप्टोकरेंसी के लिए एक पीयर के रूप में सेवा करने में अधिक संभीलन है।

इस शोध प्रबंध में, हम पहले एक विकेन्द्रीकृत लॉटरी का प्रस्ताव करते हैं जिसे एक क्रिप्टोकुरेंसी नेटवर्क पर तैनात किया जा सकता है। विकेन्द्रीकृत लॉटरी को लॉटरी विजेताओं को उचित समय से पुरस्कार के लिए उच्च गति और उच्च पुरस्कार वित्तीय पारदर्शिकता तक पहुंच की आवश्यकता होती है। व्यवहारिक रूप से, एक वित्तीयी की उपस्थिति में उच्च गति नियतात्मक पारदर्शिकता प्राप्त करना पैर-तुच्छ है। तीसरा से, क्वांटम प्रोटोकॉल के माध्यम से सर्वरों पुरानी बाइजेंटी एप्लीकेट (बीजान्टिन एप्लीकेट) समस्या को फिर से देखना इस आवश्यकता के लिए एक समाधान प्रदान करता है। सैद्धांतिक विकेन्द्रीकृत लॉटरी समाधान विकसित करने के लिए हम ब्लॉकचेन सार्वजनिकी और क्वांटम बाइजेंटी समझौते दोनों का लाभ उठाते हैं।

वितरित सिस्टम अनुप्रयोग के लिए ब्लाक की एक और समस्या (और दुनिया भर के नियामक निकायों के लिए कोई छोटा उपाय नहीं है) अनुप्रयुक्त क्रिप्टोकरेंसी के ब्लॉकचेन सार्वजनिकी के हिस्से के रूप में कानूनी लेनदेन का प्रसंस्करण और पुष्टि है। यह आवश्यक है कि सभी क्रिप्टोकुरेंसी लेनदेन संप्रभु क्षेत्राधिकार के कानूनी नियमों के अनुरूप हों, जिसके भीतर उन्हें प्रसंस्करित किया गया है। इस प्रकार, विभिन्न संप्रभु व्यवस्थाओं के वित्तीय नियामकों को क्रिप्टोकरेंसी लेनदेन की संरचना और वैधता में एक कहना चाहिए। दूसरे शब्दों में कहा गया है, इस क्रिप्टोकरेंसी ब्लॉकचेन में कानूनी लेनदेन के सेट को अधिकतम करने के लिए एक आम सहमति आधारित नियामक संरचना और एक सैद्धांतिक प्रणाली प्रदान करते हैं। हमारा तरीका पिछली नियामक नीतियों से बिल्कुल अलग है, क्योंकि यह ब्लॉकचेन सिस्टम में कुल वित्तीयकृत आय सहमति संरचना के एक कार्य के रूप में कानूनी लेनदेन सेट को अधिकतम करता है।

Contents

List of Figures

List of Acronyms

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

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