palgrave pivot

The Economics of Blockchain Consensus

Exploring the Key Tradeoffs in Blockchain Design

Joshua Gans

palgrave macmillan

The Economics of Blockchain Consensus

Joshua Gans

The Economics of Blockchain Consensus

Exploring the Key Tradeoffs in Blockchain Design

palgrave
macmillan

Joshua Gans
Rotman School of Management
University of Toronto
Toronto, ON, Canada

ISBN 978-3-031-33082-7 ISBN 978-3-031-33083-4 (eBook)
https://doi.org/10.1007/978-3-031-33083-4

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Acknowledgements

Special thanks to Eric Budish, Ethan Buchman, Agostino Capponi, Scott Kominers Scott Stornetta and Richard Titus for helpful discussions. I owe a great debt to my co-authors on blockchain research: Christian Catalini, Neil Gandal, Guillaume Haeringer, Hanna Halaburda and Richard Holden. I also want to acknowledge Tim Roughgarden, whose video series on the Foundations of Blockchain helped me navigate a dense literature.

Contents

1 Introduction 1
References 7

2 The Value of Blockchain Consensus 9
2.1 Defining Blockchains 10
Ledgers 10
Distributed Ledgers 11
Blocks of Transactions 12
How to Timestamp a Digital Document 13
Distributed Blockchain Networks 16
2.2 The Driver of Value 16
Trust 17
Enforceable Contracts 19
Cheap Verification 20
Cryptocurrencies: Verification-Enabled Payments 22
2.3 Consensus and Trust 23
References 26

3 Security Versus Speed 27
3.1 Byzantine Fault Tolerance 29
Idealised Environment 30
Malicious Nodes 32
No Digital Signatures 35
Asynchronous Networks 38

What Determines the Power of Malicious Actors? 40
Summarising the Trade-Off 42
3.2 The Longest Chain Rule 43
The Mechanics of LCR Coordination 44
Block Finality 46
3.3 Conclusion 48
References 49

4 Permissioned Versus Permissionless 51
4.1 Bitcoin Proof of Work 53
4.2 Permissionless Leader Selection 54
4.3 Attacks on Permissionless Blockchains 56
The Costs of a Double-Spend Attack 57
4.4 Comparison with Permissioned Network 61
Transaction Safety in a Permissioned Network 62
Comparison 63
Cost Incidence 63
4.5 Conclusion 64
References 66

5 Proof of Work Versus Proof of Stake 69
5.1 Proof of Stake in a Permissionless Environment 70
A Longest Chain Rule Approach 71
A BFT Approach 75
5.2 Comparison with Proof of Work 78
References 83

6 Cryptography Versus Incentives 85
6.1 Blockchain Front-Running 86
6.2 A Model of Front-Running 88
6.3 Using Cryptography 90
6.4 A Mechanism to Deter Front-Running 91
The Need to Discretise Time 92
The Single Legitimate Claimant Case 92
Further Issues 95
The Multiple Legitimate Claimant Case 96
Implementation Choices 97
6.5 Conclusion 99
References 100

7 Rules Versus Mechanisms 103
7.1 What Is Blockchain Truth? 104
7.2 Mechanism for Byzantine Fault Tolerance 106
A Simultaneous Report Mechanism 107
Robustness to Multi-node Attacks 110
7.3 Mechanism to Resolve Forks 111
A Solomonic Mechanism 112
7.4 Conclusion 115
References 116

References 117

Index 123

List of Figures

Fig. 1.1 Trade-offs between security and speed 6
Fig. 2.1 Updating the ledger 10
Fig. 2.2 A blockchain 12
Fig. 2.3 Contracting game between *A* and *B* 17
Fig. 3.1 Forked blockchain 44
Fig. 6.1 Assembling competing claims 93

CHAPTER 1

Introduction

Abstract This chapter discusses the intertwined origins of economics and computer science, highlighting the invention of the blockchain by the mysterious Satoshi Nakamoto. The chapter emphasises the importance of Nakamoto's innovation in creating a distributed ledger system, the permissionless blockchain, that requires no trust relationships. The chapter also delves into the economic implications of cryptocurrencies, arguing that tokens are essential to the operation of decentralised systems. The intention is to explore the inner workings of blockchain consensus and to make this literature more accessible to economists. The book focuses on trade-offs, such as security versus speed, and permissioned versus permissionless networks, and examines the incentives behind Proof of Work and Proof of Stake blockchains.

Keywords Economics · Computer science · Blockchain · Nakamoto · Consensus

For as long as there has been economics and computer science, there has been a relationship between the two disciplines. Charles Babbage was a leading economist who developed a theory of the division of cognitive labour (Babbage, 1832) before turning to invent the first

J. Gans, *The Economics of Blockchain Consensus*,
https://doi.org/10.1007/978-3-031-33083-4_1

computer, the Analytical Engine. John von Neumann famously developed the theory of games (Von Neumann & Morgenstern, 1944) and contributed to growth theory before developing the hardware/software design for modern computers. Herbert Simon won a Nobel prize in economics for his theory of bounded rationality and a Turing Award in computer science for his advances in developing artificial intelligence. So perhaps it should be no surprise that the computer science of operating distributed networks should receive a significant advance from the same person (the still unknown Satoshi Nakamoto [2008]) who cracked the problem of how to launch a digital currency. But just over a decade and a half ago, that happened, and most were surprised.

The common origins of economics and computer science have diverged over the years. This is why Nakamoto's innovation was so surprising. The challenge was to build a distributed network that did not require pre-registration or trust in the nodes that operated it. Nakamoto showed how to take three separate computer science innovations—the blockchain, cryptography and the notion of Proof of Work—and combine them to construct a permissionless blockchain, a distributed ledger that required no trust relationships to reach a consensus as to what the contents of the ledger were.

But what motivated Nakamoto was not an advance in computer science but instead an advance in monetary economics. Money had gone digital some decades ago. While cash-on-hand is a key part of the economy, most of the ways we use money are by sending messages from one bank to another to debit and credit different accounts accordingly. The banks then keep their own records along with a series of regulations to ensure they do not take advantage of their position to create too much money out of thin air. For Nakamoto, however, there was concern about the privileged position of the banks themselves. And in 2008, there was ample reason not to trust them as holders of the monetary system as the world was in the midst of its biggest financial crisis since the Great Depression of the 1930s.

Nakamoto had realised that it was the record-keeping part of the monetary economy that needed to be preserved but that no clear and anointed institution should be the one preserving it. Indeed, anyone, anywhere, with a computer could play their part. By embedding some rules in code that could not be changed without a broad consensus, Nakamoto showed that digital tokens (which were names bitcoins) could be created and allocated to different users securely in cryptographically

locked wallets. The wallets were just entries on a ledger. But importantly, those with tokens registered to them would be the only ones able to move those tokens from their own wallet to someone else on the registry. In economics, Narayana Kocherlakota (1998) had demonstrated that money could be represented as entries in a ledger in a way that could operate as a memory to account for productive activity in the economy. Kocherlakota was talking theoretically. Bitcoin, when it emerged, was that theory becoming a reality.

Economists have struggled to understand how seemingly valuable digital tokens could just be created by code and, at the very least, come to behave like financial assets that have some, at least purported, relationship to the real economy. But it is safe to say that deep down, economists always knew money could just come into being; in particular, Keynes (1937) and Fama (1980). The task of understanding cryptocurrencies is far from done in economics. But it is important to recognise that Nakamoto's contribution was unprecedented. In just nine pages (well, eight plus references), an important branch of both fields was revolutionised.

I am an economist who has been interested in these developments; although not in any way that would have allowed me to obtain some share of the riches as cryptocurrency went from nothing to something. But the weeds of Nakamoto's innovation have intrigued me. Setting aside the monetary aspects of all of this, the idea that it would be possible to create sustainable and distributed ledgers of anything under the guise of what we now term 'blockchain technologies' seemed to offer the potential for streamlining so many institutions; in particular, those around contracting (Catalini & Gans, 2020; Gans, 2022). This is perhaps the attitude of what many like to claim their interest in these technologies are—'blockchain, not bitcoin'—but I have come to believe that the token aspects developed by Nakamoto and others cannot be separated from the vision of a decentralised ledger that might be applied to matters beyond money. Instead, the tokens themselves and their exchangeability with the 'real world' (Gans & Halaburda, 2015) play a key role in financing the operation of decentralised systems. If you want those systems to be permissionless, there is no separating them.

Thus, arises this book. My intention is to steer away from the monetary and financial aspects of cryptocurrencies. Instead, I want to look at the inner workings of the blockchain consensus that is at the heart of it all. Those developments have, to date, largely lay with computer science. That