

Book Description:

Bitcoin and Cryptocurrency Technologies provides a comprehensive introduction to the revolutionary yet often misunderstood new technologies of digital currency. Whether you are a student, software developer, tech entrepreneur, or researcher in computer science, this authoritative and self-contained book tells you everything you need to know about the new global money for the Internet age. How do Bitcoin and its block chain actually work? How secure are your Bitcoins? How anonymous are their users? Can cryptocurrencies be regulated? These are some of the many questions this book answers. It begins by tracing the history and development of Bitcoin and cryptocurrencies, and then gives the conceptual and practical foundations you need to engineer secure software that interacts with the Bitcoin network as well as to integrate ideas from Bitcoin into your own projects. Topics include decentralization, mining, the politics of Bitcoin, altcoins and the cryptocurrency ecosystem, the future of Bitcoin, and more. * An essential introduction to the new technologies of digital currency* Covers the history and mechanics of Bitcoin and the block chain, security, decentralization, anonymity, politics and regulation, altcoins, and much more* Features an accompanying website that includes instructional videos for each chapter, homework problems, programming assignments, and lecture slides* Also suitable for use with the authors' Coursera online course* Electronic solutions manual (available only to professors)

Table of Contents

Preface		vii
Foreword	The long Road to Bitcoin Jeremy Clark	ix
Chapter 1	Introduction to Cryptography and Cryptocurrencies	01
Chapter 2	How Bitcoin Achieves Decentralization	27
Chapter 3	Mechanics of Bitcoin	51
Chapter 4	How to store and Use Bitcoins	76
Chapter 5	Bitcoin Mining	104
Chapter 6	Bitcoin and Anonymity	138
Chapter 7	Community, Politics and Regulation	168
Chapter 8	Alternative Mining Puzzles	190
Chapter 9	Bitcoin as a Platform	213
Chapter 10	Altcoins and the Cryptocurrency Ecosystem	242
Chapter 11	Decentralized Institutions: The Future of Bitcoin?	272
Conclusion		286

Acknowledgements	287
About Authors	289
Index	291

About Author:

Arvind Narayanan (phD 2009) is an Assistant Professor of computer scientist at Princeton. Narayanan leads the Princeton Web Transparency and Accountability Project that aims to uncover how companies are collecting and using our personal information. He also leads a research group studying the security, anonymity and stability of Bitcoin and cryptocurrencies. His doctoral research showed that data anonymization is broken in fundamental ways, for which he jointly received the 2008 privacy enhancing Technologies Award.