Preface

The question of how one party can transfer money to another party without physically exchanging money is an old problem. The most common solution, available for hundreds of years, is to use a trusted third party, like a bank. If a bank is mutually trusted and has custody of one person's money, this person can write a check or by some other means direct the bank to pay their counterparty. A check can be thought of as simply instructions for the money's custodian to do something with the money.

Such relationships require trust. If the two parties do not use the same bank, there must be a relationship between the banks. If the banks are in different jurisdictions, this can be an obstacle.

For many reasons, individuals may want to transmit money without the use of a trusted third party. They may want to do this at a distance. They may also want to do this with some level of anonymity. Suppose a network of individuals forms around this goal: to be able to send money to each other, without doing so in person. Keeping in mind the notion of a bank cashing a check, there are issues that must be overcome:

– There must be a way for everyone involved in the network to know what money is good, at any given time.
– Parties must be able to "sign" payments in a verifiable way. That is, there must be some way to verify that the instructions to transfer money are coming from the owner of the money.
– There must be a way to ensure that a payment is not reused repeatedly.

Cryptography (a subdiscipline of number theory) solves the second issue quite handily. A blockchain attempts to solve the other two problems, with probabilistic assurances.

The goal of this text is to offer some accessible game-theoretic background for analysis of proof-of-work blockchains. Much of the current game-theoretic understanding is found in podcasts, videos, blog posts, and uncurated forum discussions and is poorly formalized. On the other hand, quite a bit of academic research exists, but much is esoteric and not written with immediate applications in mind. This textbook is a brazen attempt to bridge this gap. Deeper game-theoretic issues are discussed at length with the goal that an undergraduate student can understand their applicability.

The background material provided in the first three chapters includes an overview of how proof of work functions, followed by an overview of basic concepts from probability theory and relevant notions from game theory. In the remainder we will discuss the implication for Bitcoin.

This textbook began as a syllabus for the Clark Honors College at the University of Oregon, proposed in February of 2020. As the material was developed it became clear that there was much more than would fit in a single-quarter undergraduate course. The current version contains material far beyond the scope of the original course and seeks to serve several purposes:

– offer a comprehensive textbook for such an upper-division university course,

https://doi.org/10.1515/9783110772845-201

- establish a foundational reference framework for discourse around Bitcoin's game theory,
- facilitate descriptive conversations surrounding Bitcoin, rather than the normative conversations that dominate the public discourse, and
- provide a relatively thorough reference for journalists, policy makers, and others who may have little exposure to blockchain technology but would like to understand the underpinnings of blockchain security.

I have tried to make it self-contained as much as possible. Many chapters require some understanding of college-level mathematics, some do not. Some chapters will go deep into the weeds of the mathematics, while some chapters (the final chapter, for example) offer more of a bird's-eye view.