Programming the Open Blockchain

Mastering Bitcoin

Andreas M. Antonopoulos • Second Edition

Last Revision: March 27, 2018

Table of Contents

Abstract

These notes are intended as a resource by the contributors; past, present, or future students of this course, and anyone interested in the material. The goal is to provide an end-to-end resource that covers all material discussed in the book displayed in an organized manner. If you spot any errors or would like to contribute, please contact me directly.

1 Introduction

2 How Bitcoin Works

3 Keys, Addresses

The Bitcoin protocol relies heavily on two fundamental concepts of cryptography— digital signatures (proving knowledge of a secret), and digital fingerprints (proving authenticity of data).

3.1 Introduction

Ownership of Bitcoin is established by the ownership of digital keys, Bitcoin addresses and digital signatures.

Definition 3.1. (digital keys) a private and public key pair generated and managed independently of the Bitcoin protocol that are stored locally by the user or in a simple database (wallet). Digital keys enable decentralized trust and control, ownership attestation, and the cryptographic-proof security model.

Definition 3.2. (Bitcoin address) a digital fingerprint usually generated from a public key corresponding to a user of the network; however, it is plausible that the digital fingerprint can represent deployed scripts.

Definition 3.3. (digital signature) a signature generated from a private key used to spend funds and testify ownership.

3.2 Asymmetric Cryptography

Asymmetric cryptography is used by the Bitcoin protocol to generate digital signatures. A private key is prescribed with a transaction to produce a numerical signature. This signature can only be produced with knowledge of the private key; however, anyone with access to the public key and the transaction fingerprint can use them to verify the signature (hence asymmetric). Thus, ownership and control over this private key is critical in safeguarding funds associated with the Bitcoin address.

3.3 Private Keys

A private is generated from a random 256-bit number usually encoded in Base58 checksum format. The range of addresses is fixed between the range $[1,\ n-1]$, where n is the constant $1.58 * 10^{77}$ defined as the order of the elliptic curved used by Bitcoin. It is critical to ensure sufficient 256 bits of entropy; therefore, it is suggested to used `HASH256(CSPRNG(seed))` whilst ensuring the output iss less than $n-1$.

3.4 Public Keys

Elliptic Curve Cryptography

Generating a Public Key

3.5 Addresses

Base58 and Base58Check Encoding

Key Formats

3.6 Advanced Key and Addresses

Encrypted Private Keys

Pay-to-Script Hash (P2PHS) and Multisig Addresses