Continue



Mastering Bitcoin is a technical book that explains what Bitcoin is and how it works. This repository contains the complete text of three editions of the book Mastering Bitcoin as published in paperback and ebook formats by O'Reilly Media. Different editions are covered by different open licenses. The three editions are available for free, see BOOK.md. Click on each chapter to read in your browser. Some links may not work when reading on Github because they are intended for print and ebook editions and require all chapters to be rendered together. Github cannot render the complete book at once. "Mastering Bitcoin: Programming the Open Blockchain (3rd Edition)" is now available in paperback and ebook formats by many booksellers worldwide. It is licensed under Creative Commons Attribution-ShareAlike 4.0 International License. The first print of Mastering Bitcoin was published by O'Reilly Media in December 2023. Mastering Bitcoin: Programming the Open Blockchain (Third Edition) by Andreas M. Antonopoulos and David A. Harding is a great technical guide to blockchain technology. It explains complex subjects in an easy-to-understand way, making it accessible to everyone. The book has three editions, each with its own open license. The first edition was published by O'Reilly Media in 2014 and is widely considered the best technical guide to Bitcoin ever written. Andreas M. Antonopoulos is a renowned expert in blockchain technology and has authored several books, including Mastering Bitcoin and The Internet of Money.Mastering Bitcoin is written by Andreas M. Antonopoulos and provides essential knowledge for participants in the internet of money. The book has become a bestseller on Amazon, and its follow-up books, Mastering Ethereum Volume Two and Mastering Lightning Network are also successful titles. In 2018, Mastering Ethereum was published, followed by another technical guide to the Ethereum network. The book explains Bitcoin's second layer payment network, called Lightning Network. Andreas has written several articles about Bitcoin, is a permanent host on the Speaking of Bitcoin Podcast, and frequently speaks at technology conferences worldwide. He serves as an advisor to bitcoin companies, founded businesses, and launched community open-source projects. As for reading the book Mastering Bitcoin, one must first get familiar with the internet of money. The book covers topics such as blockchain applications, security principles, and how to combine building blocks into higher-level applications. The second edition includes detailed information on bitcoin's decentralized network, transaction lifecycle, peer-to-peer architecture, and user stories illustrating key technical concepts. Bitcoin development environment is another topic discussed in the book, including compiling Bitcoin Core from the source code and selecting a suitable release version.on the Bitcoint Core Client StatusExploring and Decoding TransactonsExploring BlocksUsing Bitcoint Core’s Programmatic InterfaceAlternative Clients, Libraries, and ToolkitsC/C++JavaScriptJavaPHPPythonRubyGoRustC#Objective-CIntroductionPublic Key Cryptography and CryptocurrencyPrivate and Public KeysPrivate KeysPublic KeysElliptic Curve Cryptography ExplainedGenerating a Public KeyBitcoin AddressesBase58 and Base58Check EncodingKey FormatsImplementing Keys and Addresses in C++Implementing Keys and Addresses in PythonAdvanced Keys and AddressesEncrypted Private Keys (BIP-38)Pay-to-Script Hash (P2SH) and Multisig AddressesVanity AddressesPaper WalletsWallet Technology OverviewNondeterministic (Random) WalletsDeterministic (Seeded) WalletsHD Wallets (BIP-32/BIP-44)Seeds and Mnemonic Codes (BIP-39)Wallet Best PracticesUsing a Bitcoin WalletWallet Technology DetailsMnemonic Code Words (BIP-39)Creating an HD Wallet from the SeedUsing an Extended Public Key on a Web StoreIntroductionTransactions in DetailTransactions—Behind the ScenesTransaction Outputs and InputsTransaction OutputsTransaction InputsTransaction FeesAdding Fees to TransactionsTransaction Scripts and Script LanguageTuring IncompletenessStateless VerificationScript Construction (Lock + Unlock)Pay-to-Public-Key-Hash (P2PKH)Digital Signatures (ECDSA)How Digital Signatures WorkVerifying the SignatureSignature Hash Types (SIGHASH)ECDSA MathThe Importance of Randomness in SignaturesBitcoin Addresses, Balances, and Other AbstractionsIntroductionMultisignaturePay-to-Script-Hash (P2SH)P2SH AddressesBenefits of P2SHRedeem Script and ValidationData Recording Output (RETURN)TimelocksTransaction Locktime (nLocktime)Check Lock Time Verify (CLTV)Relative TimelocksRelative Timelocks with nSequenceRelative Timelocks with CSVMedian-Time-PastTimelock Defense Against Fee SnipingScripts with Flow Control (Conditional Clauses)Conditional Clauses with VERIFY OpcodesUsing Flow Control in ScriptsComplex Script ExampleSegregated WitnessWhy Segregated Witness?How Segregated Witness WorksSoft Fork (Backward Compatibility)Segregated Witness Output and Transaction ExamplesUpgrading to Segregated WitnessSegregated Witness’ New Signing AlgorithmEconomic Incentives for Segregated WitnessPeer-to-Peer Network ArchitectureNode Types and RolesThe Extended Bitcoin NetworkBitcoin Relay NetworksNetwork DiscoveryFull NodesExchanging “Inventory”Simplified Payment Verification (SPV) NodesBloom FiltersHow Bloom Filters WorkHow SPV Nodes Use Bloom FiltersSPV Nodes and PrivacyEncrypted and Authenticated ConnectionsTor TransportPeer-to-Peer Authentication and EncryptionTransaction PoolsIntroductionStructure of a BlockBlock HeaderBlock Identifiers: Block Header Hash and Block HeightThe Genesis BlockLinking Blocks in the BlockchainMerkle TreesMerkle Trees and Simplified Payment Verification (SPV)Bitcoin’s Test BlockchainsTestnet—Bitcoin’s Testing PlaygroundSegnet—The Segregated Witness TestnetRegtest—The Local BlockchainUsing Test Blockchains for DevelopmentIntroductionBitcoin Economics and Currency CreationDecentralized ConsensusIndependent Verification of TransactionsMining NodesAggregating Transactions into BlocksThe Coinbase TransactionCoinbase Reward and FeesStructure of the Coinbase TransactionCoinbase DataConstructing the Block HeaderMining the BlockProof-of-Work AlgorithmTarget RepresentationRetargeting to Adjust DifficultySuccessfully Mining the BlockValidating a New BlockAssembling and Selecting Chains of BlocksBlockchain ForksMining and the Hashing RaceThe Extra Nonce SolutionMining PoolsConsensus AttacksChanging the Consensus RulesHard ForksHard Forks: Software, Network, Mining, and ChainDiverging Miners and DifficultyContentious Hard ForksSoft ForksCriticisms of Soft ForksSoft Fork Signaling with Block VersionBIP-34 Signaling and ActivationBIP-9 Signaling and ActivationConsensus Software DevelopmentSecurity PrinciplesDeveloping Bitcoin Systems SecurelyThe Root of TrustUser Security BestRewritten text with selected method SE (40% probability)