27th November, 2022

NITDA Blockchain Scholarship 2022

Curriculum Overview

- Introduction to JavaScript
- Introduction to Golang
- Introduction to Bitcoin Theory
- Bitcoin Enterprise
- Bitcoin Protocol and design
- Hash functions
- Merkle Tree
- Digital Signatures
- Bitcoin Development
- Bitcoin Scripts

Introduction to Bitcoin Theory

Course Overview

Bitcoin Theory covers the design of Bitcoin as a system as prescribed by Satoshi Nakamoto. This course is open to anyone who is interested in Bitcoin and is the beginner course in this series. Some technical experience would be helpful to complete the course, however it is open to anyone regardless of experience.

***Chapters*: 13**
***Duration*: 9 Hours**
***Difficulty*: Beginner**

Course Outline

- **Chapter 1: Abstract (Approx 45 mins)**
    - 00 Abstract read-through
    - 01 Peer-to-peer cash
    - 02 Digital signatures and trusted third parties
    - 03 Abstract Assessment No.1
    - 04 Peer to Peer network
    - 05 Time Chain and Proof of Work
    - 06 CPU Power
    - 07 Abstract Assessment No.2
    - 08 Cooperation in the network
    - 09 Network structure
    - 10 Messaging between nodes
    - 11 Abstract Video
    - 12 Abstract Assessment No.3

- **Chapter 2: Introduction (Approx 45 mins)**
    - 00 Introduction read-through
    - 01 Commerce on the internet
    - 02 Non reversible transactions
    - 03 Introduction Assessment No.1
    - 04 Privacy in commerce
    - 05 The paradigm of fraud acceptance
    - 06 What is needed…
    - 07 Introduction Assessment No.2
    - 08 Protecting sellers from fraud
    - 09 Proposed solution
    - 10 Security and honesty
    - 11 Introduction Video
    - 12 Introduction Assessment No.3

- **Chapter 3: Transactions (Approx 45 mins)**
    - 00 Section read-through
    - 01 Electronic Coins
    - 02 Spending a coin
    - 03 Transactions Assessment No.1
    - 04 Payee verification
    - 05 Existing solutions
    - 06 First Seen Rule
    - 07 Transactions Assessment No.2
    - 08 Broadcasting Transactions
    - 09 Achieving Consensus
    - 10 Proof of acceptance
    - 11 Transactions Video
    - 12 Transactions Assessment No.3

- **Chapter 4: Timestamp Server (Approx 15 mins)**
    - 00 Section read-through
    - 01 Timestamped Hashes
    - 02 A chain of timestamped hashes
    - 03 Timestamp Server Video
    - 04 Timestamp Server Assessment No.1

- **Chapter 5: Proof of Work (Approx 60 mins)**
    - 00 Section read-through
    - 01 Hashcash
    - 02 Scanning random space
    - 03 Proof of Work Assessment No.1
    - 04 Nonce
    - 05 Immutable Work
    - 06 Chained effort
    - 07 Proof of Work Assessment No.2
    - 08 One CPU, one vote
    - 09 The majority decision
    - 10 The honest chain
    - 11 Proof of Work Assessment No.3
    - 12 Attacking the longest chain
    - 13 Controlling the block discovery rate
    - 14 Proof of Work Video
    - 15 Proof of Work Assessment No.4

- **Chapter 6: Network (Approx 45 mins)**
    - 00 Section read-through
    - 01 Running the Network
    - 02 Network Assessment No.1
    - 03 The longest chain
    - 04 Simultaneous blocks
    - 05 Network Assessment No.2

  - 06 Breaking the tie
  - 07 Missed messages
  - 08 Network Video
  - 09 Network Assessment No.3

- **Chapter 7: Incentive (Approx 45 mins)**
  - 00 Section read-through
  - 01 The Coinbase Transaction
  - 02 Coin Distribution
  - 03 Incentive Assessment No.1
  - 04 Mining analogy
  - 05 Transaction fees
  - 06 The end of inflation
  - 07 Incentive Assessment No.2
  - 08 Encouraging honesty
  - 09 The attacker’s dilemma
  - 10 Incentive Video
  - 11 Incentive Assessment No.3

- **Chapter 8: Reclaiming Disk Space (Approx 30 mins)**
  - 00 Section read-through
  - 01 Spent transactions
  - 02 The Merkle Tree
  - 03 Reclaiming Disk Space Assessment No.1
  - 04 Compacting blocks
  - 05 Block Headers
  - 06 Reclaiming Disk Space Video
  - 07 Reclaiming Disk Space Assessment No.2

- **Chapter 9: Simplified Payment Verification (Approx 45 mins)**
  - 00 Section read-through
  - 01 Full network nodes

  - 02 Merkle Branches
  - 03 Simplified Payment Verification Assessment No.1
  - 04 Transaction acceptance
  - 05 Verification during attack situations
  - 06 Maintaining an attack
  - 07 Simplified Payment Verification Assessment No.2
  - 08 Invalid Block Relay System
  - 09 Businesses running nodes
  - 10 Simplified Payment Verification Video
  - 11 Simplified Payment Verification Assessment No.3

- **Chapter 10: Combining and Splitting Value (Approx 30 mins)**
  - 00 Section read-through
  - 01 Dynamically sized coins
  - 02 Inputs and Outputs
  - 03 Combining and Splitting Value Assessment No.1
  - 04 A typical example
  - 05 Fan-out
  - 06 Combining and Splitting Value Video
  - 07 Combining and Splitting Value Assessment No.2

- **Chapter 11: Privacy (Approx 45 mins)**
  - 00 Section read-through
  - 01 Traditional Models
  - 02 Privacy in Bitcoin
  - 03 Privacy Assessment No.1
  - 04 Public records
  - 05 Stock Exchange Comparison
  - 06 Key Re-use
  - 07 Privacy Assessment No.2
  - 08 Linking inputs
  - 09 Linking the owner

  - 10 Privacy Video
  - 11 Privacy Assessment No.3

- **Chapter 12: Calculations (Approx 60 mins)**
  - 00 Section read-through
  - 01 Attacking the chain
  - 02 Things the attacker cannot achieve…
  - 03 The only thing the attacker can achieve…
  - 04 The Binomial Random Walk
  - 05 The Gambler’s Ruin
  - 06 Exponential odds
  - 07 Waiting for confirmation…
  - 08 Attack via proof of work
  - 09 Vanishing probabilities
  - 10 Calculations Video
  - 11 Calculations Assessment No.1

- **Chapter 13: Conclusion (Approx 15 mins)**
  - 00 Section read-through
  - 01 Conclusion
  - 02 Conclusion Video

- **Bitcoin Theory Final Assessment**

Bitcoin Enterprise

Course Overview

This course is targeted at C-Level executives and who are seeking to build next generation platforms using Bitcoin as a technology substrate. The purpose of this course is to give answers to questions such as:

1. What is the difference between BSV and Cryptocurrency?
2. What are blocks
3. What are transactions
4. Separation of blockchain vs transaction ledger
5. Working blockchain - Pruning vs SPV and block linked databases
6. Why fixed protocol
7. What is a 'private blockchain'?
8. Why is Proof of Work superior vs Proof of Stake/Authority/ETC
9. Why is proof of work inefficient for BTC but efficient for BSV and more efficient at scale?
10. What do I need to understand to start working out how to leverage Bitcoin

***Chapters*: 3**
***Duration*: 1.5 Hours**
***Difficulty*: Beginner**

Course Outline

- **Chapter 1: About BitcoinSV**
    - 00 Introduction
    - 01 Safe, Instant Transactions at a Predictably Low Cost
    - 02 Scalability to Accommodate Global Demand
    - 03 A Plan for Regulatory Acceptance
    - 04 Protocol Stability

- **Chapter 2: Technical Details**
    - 00 The Network
    - 01 The Bitcoin Satoshi Vision Node Client
    - 02 The Protocol - Simple, Robust and Unbounded
    - 03 Proof of Work
    - 04 Privacy and Identity
    - 05 Permissions, Privacy and the Metanet

- **Chapter 3: Resources and Tools**
    - 00 The Technical Standards Committee
    - 01 The Working Blockchain
    - 02 The Metanet and the new Internet of Value

Bitcoin Basics: Protocol and design

Course Overview

This course serves as an introduction to the Bitcoin protocol, its method of operation and is intended for beginners to Bitcoin.

***Chapters*: 5**
***Duration*: 3 Hours**
***Difficulty*: Beginner**

Course Outline

- **Chapter 1: Introduction**
    - 00 Chapter Introduction
    - 01 What is Bitcoin?
    - 02 Bit-Coin

- **Chapter 2: The Bitcoin Ledger**
    - 00 Chapter Introduction
    - 01 The Ledger
    - 02 Triple Entry Accounting
    - 03 Example
    - 04 The Bitcoin Ledger Assessment

- **Chapter 3: Coins and Transactions**
    - 00 Chapter Introduction
    - 01 Coins

  - 02 Transactions
  - 03 Transaction Fees
  - 04 Coins and Transactions Assessment

- **Chapter 4: Theory**
  - 00 Chapter Introduction
  - 01 White Paper Sections
  - 02 Theory Assessment

- **Chapter 5: Conclusion**

Bitcoin Primitives: Hash functions

Course Overview

There are three primitive elements found in Bitcoin: Hash Functions, Merkle Trees, and Digital Signatures. If you take the time to learn these three Bitcoin primitives well, you will likely find the learning curve to understanding Bitcoin significantly reduced. The focus of this course is Hash functions.

We examine what hash functions are, the hash functions used in Bitcoin, how hash functions are used in Bitcoin, why double hashing is used in Bitcoin, and the role hash functions play in Bitcoin's security model. Bitcoin makes use of two hash functions: SHA-256 and RIPEMD-160.

There is example code in various parts of the course, and two example hash function implementations all written using the Go programming language. These examples are simply meant to aid in understanding the course material; knowing how to read and write code is not required to complete this course.

However, although it is not necessary to understand and complete the course, some familiarity with command line or terminal environments and programming is assumed with respect to the example code presented in the course.

Installation of Supporting Libraries Quick-Start: GoLang

You can install Go for your operating system from the official Go website: https://go.dev/doc/install

Once you have Go installed, create a new directory and initialize a new Go module using the following command:

```
go mod init github.com/[your username]/bsv-examples
```

The examples in this course also utilize the official BSV libsv Go libraries which you can add to your module using the following commands:

```
go get github.com/libsv/go-bt
go get github.com/libsv/go-bk
go get github.com/libsv/go-bc
```

The GoLang code used in this course can be found here:
https://github.com/jakeBitcoinAssociation/hash-functions

Chapters: 7
Duration: 5 Hours
Difficulty: Beginner

Course Outline

- **Chapter 1: What are Hash Functions?**
    - 00 What are Hash Functions?
    - 01 The Differences Between Hashing and Encryption
    - 02 The Three Important Properties of Hash Functions
    - 03 The Hash Functions Found in Bitcoin
    - 04 What are Hash Functions Assessment

- **Chapter 2: Base58 and Base58Check**
    - 00 What is Base58 and Why Does Bitcoin Use It?
    - 01 What is Base58Check and How Does Bitcoin Use It?
    - 02 Base58 and Base58Check Assessment

Bitcoin Primitives: Merkle Trees

Course Overview

There are three foundational concepts, if understood well, can make the initial learning journey for Bitcoin SV easier. We call them the Bitcoin primitives. While the other two concepts are Hash Functions and Digital signatures, the focus of this course is to cover Merkle trees. As this is a beginner-level course, it assumes no knowledge of Bitcoin SV. This Course is designed for anyone that wants to learn more about Bitcoin and will introduce some general computer science techniques. Upon completion students will understand how these techniques enable the system to scale efficiently.

At the end of the course you will understand the following:

1. What Merkle trees are.
2. How Merkle trees are used in Bitcoin.
3. Why Merkle trees are used in Bitcoin
4. How Merkle trees help Bitcoin scale.
5. What elements are involved in a Standardized Merkle Proof.

***Chapters*: 6**
***Duration*: 4 Hours**
***Difficulty*: Beginner**

Course Outline

- **Chapter 1: The Merkle Tree**
  - 00 What is a Merkle Tree?
  - 01 Why Use a Merkle Tree?

  - 02 Merkle Trees in Action
  - 03 The Merkle Tree Assessment

- **Chapter 2: Merkle Trees in Bitcoin**
  - 00 The Data Elements
  - 01 Transaction Merkle Trees
  - 02 Transaction Merkle Trees in Action
  - 03 Merkle Trees in Bitcoin Assessment

- **Chapter 3: Merkle Trees and the Block Header**
  - 00 What is the Block Header
  - 01 The Hash Puzzle
  - 02 Proof of Work in Action
  - 03 Merkle Trees and the Block Header Assessment

- **Chapter 4: Merkle Trees and Verifying Proof-of-Work**
  - 00 Broadcasting the Block
  - 01 The Coinbase Transaction
  - 02 Data Integrity of the Block
  - 03 Saving Disk Space
  - 04 Merkle Trees and Verifying Proof-of-Work Assessment

- **Chapter 5: Standardized Merkle Proofs**
  - 00 What is a Merkle Proof?
  - 01 The Standardized Merkle Proof
  - 02 Simple and Composite Proofs
  - 03 Standardized Merkle Proofs Assessment

- **Chapter 6: Merkle Trees and Simplified Payment Verification**
  - 00 SPV
  - 01 Offline Payments
  - 02 Merkle Trees and Simplified Payment Verification Assessment

- **Merkle Trees Final Assessment**

Bitcoin Primitives: Digital Signatures

Course Overview

Overall, there are three foundational concepts that, if understood well, can make the initial learning journey for Bitcoin SV much easier. While the two other concepts are Hash Functions and Merkle Trees, the focus of this course is to cover the third concept - Digital Signatures.

As this is a beginner-level course, it assumes no knowledge of Bitcoin SV. There are many well-proven Digital Signature Schemes such as RSA (based upon the name of its inventors Rivest-Shamir-Addlemen), Digital Standard Signature, ECDSA (Elliptic Curve Digital Signature Algorithm), used by enterprise products. For the scope of this course, our focus will only be on ECDSA as used in Bitcoin SV. In order to build a solid conceptual understanding, the course will progress in the following order:

Chapter 1 - What are Digital Signatures?
Chapter 2 - ECDSA Prerequisites
Chapter 3 - ECDSA
Chapter 4 - Bitcoin and Digital Signatures

***Chapters*: 4**
***Duration*: 3 Hours**
***Difficulty*: Beginner**

Course Outline

- **Chapter 1: What are Digital Signatures?**
    - 00 Background & Introduction
    - 01 Digital Signatures Protocol
    - 02 Properties of Digital Signatures
    - 03 What Are Digital Signatures Assessment

- **Chapter 2: ECDSA Prerequisites**
    - 00 Modular Arithmetic
    - 01 Groups, Ring, and Finite Fields
    - 02 Discrete Logarithm Problem
    - 03 Elliptic Curve Cryptography (ECC)
    - 04 Discrete Logarithm Problem with Elliptic Curves
    - 05 ECDSA Prerequisites Assessment

- **Chapter 3: ECDSA**
    - 00 Introduction
    - 01 ECDSA
    - 02 Further Discussion
    - 03 ECDSA Assessment

- **Chapter 4: Bitcoin and Digital Signatures**
    - 00 Introduction
    - 01 Bitcoin Transaction
    - 02 ECDSA (secp256k1) for Bitcoin Transaction
    - 03 Summary
    - 04 Signed Messages
    - 05 Miner Identification and Digital Signatures
    - 06 Bitcoin and Digital Signatures Assessment

- **Digital Signatures Final Assessment**

Bitcoin Development

Course Overview

Bitcoin Development focuses on the formative skills and crucial concepts to successfully build applications with Bitcoin.

***Chapters**: 8*
***Duration**: 10 Hours*
***Difficulty**: Beginner*

Course Outline

- **Chapter 1: Understanding Bitcoin**
    - 00 Chapter Introduction
    - 01 The Bitcoin Protocol
    - 02 Bit and Coin: Key Concepts
    - 03 Understanding Bitcoin Assessment No.1
    - 04 Bitcoin Ledger as a Data Store
    - 05 Unique Properties of Bitcoin Ledger
    - 06 Understanding Bitcoin Assessment No. 2
    - 07 Wallets
    - 08 Using Block Explorer
    - 09 Application Development with Bitcoin
    - 10 Understanding Bitcoin Assessment No.3
    - 11 Understanding Bitcoin Final Assessment

- **Chapter 2: Deep Dive into Basics**
  - 00 Chapter Introduction
  - 01 Background and Concepts
  - 02 Points and Elliptic Curves
  - 03 Deep Dive into Basics Assessment No. 1
  - 04 Hash Functions
  - 05 Keys and Address
  - 06 Deep Dive into Basics Assessment No. 2
  - 07 ECDSA, Signing and Verification
  - 08 Transaction Format and Script
  - 09 Creating Transactions
  - 10 Deep Dive into Basics Assessment No. 3
  - 11 Deep Dive into Basics Final Assessment

- **Chapter 3: Data Protocol: Writing to the Bitcoin Ledger**
  - 00 Chapter Introduction
  - 01 Writing to Bitcoin
  - 02 MoneyButton
  - 03 B:// - Bitcoin Data Protocol
  - 04 Writing to the Bitcoin Ledger Assessment No. 1
  - 05 Bitcom - Global Namespace Directory
  - 06 DataPay
  - 07 Writing to the Bitcoin Ledger Assessment No. 2
  - 08 TxForge
  - 09 Txpost
  - 10 Writing to the Bitcoin Ledger Assessment No. 3
  - 11 Writing to the Bitcoin Ledger Final Assessment

- **Chapter 4: Data Protocol: Reading the Bitcoin Ledger**
  - 00 Chapter Introduction
  - 01 Reading the Bitcoin Ledger
  - 02 Database on Bitcoin

  - 03 Reading the Bitcoin Ledger Assessment No. 1
  - 04 Planaria Framework
  - 05 Bitcoin Transaction Formats
  - 06 Reading the Bitcoin Ledger Assessment No. 2
  - 07 BitFS
  - 08 Bitsocket
  - 09 TXT: Semantic Bitcoin Storage
  - 10 Reading the Bitcoin Ledger Assessment No. 3
  - 11 Reading the Bitcoin Ledger Final Assessment

- **Chapter 5: Data Protocol: Advanced Protocols and Tools**
  - 00 Chapter Introduction
  - 01 Metanet: Building the new Internet
  - 02 Dealing with Files in Bitcoin Transactions
  - 03 Advanced Protocols and Tools Assessment No. 1
  - 04 Reviewing Commonly Used Data Protocols
  - 05 TXQ: Transaction Storage Queue
  - 06 Advanced Protocols and Tools Assessment No. 2
  - 07 Paypresto
  - 08 sCrypt
  - 09 Testing Bitcoin Applications
  - 10 Advanced Protocols and Tools Assessment No. 3
  - 11 Advanced Protocols and Tools Final Assessment

- **Payment Protocols**
  - 00 Chapter Introduction
  - 01 Simple Payment Verification aka SPV
  - 02 BIP270 and PayMail
  - 03 Payment Protocols Assessment No. 1
  - 04 mAPI (Merchant API)
  - 05 SPV Channels
  - 06 Payment Protocols Assessment No. 2

    - 07 Threshold Signatures and R-Puzzles
    - 08 Secret Value Distribution and HD Keys
    - 09 Operate BSV
    - 10 Payment Protocols Assessment No. 3
    - 11 Payment Protocols Final Assessment

- **Smart Contracts and Token Protocols**
    - 00 Chapter Introduction
    - 01 Electronic Contracting
    - 02 Tokens and Bitcoin
    - 03 Payment Channels and Smart Contracts
    - 04 Smart Contracts and Token Protocols Assessment No. 1
    - 05 Tokenized Protocol
    - 06 Bitcoin Computer
    - 07 Run Platform
    - 08 sCrypt Smart contracts and Tokens
    - 09 Smart Contracts and Token Protocols Assessment No. 2
    - 10 Smart Contracts and Token Protocols Final Assessment

- **Chapter 8: Conclusion and Reference Material**

- **Bitcoin Development Final Assessment**