Blockchain Innovation Program Tutorial Framework

BIP | BLOCKCHAIN INNOVATION PROGRAM

POWERED BY

BSV ACADEMY

Blockchain Innovation Program
Tutorial Framework

The Blockchain Innovation Program is a designed as an intensive 10-week programme which will provide students with educational and entrepreneurial support for them to develop a comprehensive understanding of what's involved in Bitcoin Application Development.
The programme will see the students complete the three bitcoin primitive courses Hash Functions, Merkle Trees, and Digital Signatures before they complete the newly refactored Introduction to Bitcoin Development.

Educators from the Bitcoin SV Academy team will prescribe weekly resource and question packs to stimulate the students to develop a deeper consideration for what is involved in creating a scalable Bitcoin application. The students will attend fortnightly tutorials where their answers to the question pack will be evaluated and discussed in greater detail.

Live session #1

Hash Functions	• Hash Functions and Hash Tables • Content Addressed Distributed Data Structures • Efficient Provable Data Possession for Hybrid Clouds

Course pre-requisite: Hash Functions (primitives)
Worksheet to complete prior to the live session: Week 1 – Hash Functions

Live session #2

Merkle Trees	• GitHub MerkleDAG • ForkBase: Immutable, Tamper-evident Storage • Substrate for Branchable Applications • Merkle-CRDTs - MerkleDAGs meet CRDTs • Merkle^2: A Low Latency Transparency Log System
Digital Signatures	• Digital Signatures • Legitimating Technologies: Digital Signatures Case Study. • Segwit, Mixing and Law • SigHash Flags

Course pre-requisite: Merkle Trees and Digital Signatures (Primitives)
Worksheet to complete prior to the live session: Week 2 Merkle Trees and Week 3 Digital Signatures.

Live session #3

Data and Databases	• What is DBaaS? • SQL vs NoSQL • What is Cloud Storage? • What is Object Storage? • Block vs File Storage • What is a Load Balancer? • Kubernetes vs Docker
API led Event-Driven & Microservices Architectures	• API vs SDK • What is API Management? • What is a REST API? • What is an API Gateway? • What is Event Driven Architecture? • What are Microservices? • Architecting a Cloud Native API Solution. • Blockchain Enabled Trustless API Marketplace • Unofficial API and Browser Extension Development for Augmenting Student Resources

Course pre-requisite: Bitcoin Development Chapter 1
Worksheet to complete prior to the live session: Week 4 Data and Databases and API led Event-Driven & Week 5 Microservices Architectures

Live session #4

Debunking the Blockchain Trilemma, CAP Theorem & Application Scalability	• Myths of Decentralisation • On Decentralisation • The Wizard of Blockchain • Cost Performance Trade-Off Evaluation in Microservices impacted by the CAP Theorem Limitations
Working Blockchain & Overlay Networks	• A Survey and Comparison of P2P Overlay Network Schemes. • Virtual Networking Explained • What is a Content Delivery Network • Mandala Network • SPV • Working Blockchain

Course pre-requisite: Bitcoin Development Chapter 2&3
Worksheet to complete prior to the live session: Week 6 Debunking the Blockchain Trilemma, CAP Theorem & Week 7 Application Scalability and Working Blockchain & Overlay Networks.

Live session #5

Intro to Git and Github	• Git and GitHub for Beginners • Getting Started With OpenSSH Key Management. • Setting up an Nx monorepo with Angular • Setting up CI/CD with Github Actions and Vercel
Constructing Transactions & Script	• Introduction to Bitcoin Transactions • MintBlue API, SDK and Integrations

Course pre-requisite: Bitcoin Development Chapter 4-5
Worksheet to complete prior to the live session: Week 8 Intro to Git and Github and Week 9 Constructing Transactions and Bitcoin Script.

Live session #6

Metanet	• Metanet Overlay • Dagda • The Birth of Ontology & the DAG • Tutorial on directed Acyclic Graphs • A.N.N.E preview.
End of programme	• Feedback on project completed by students • Wrap up of the programme

Course pre-requisite: Bitcoin Development Chapter 6
Worksheet to complete prior to the live session: Week 10 Metanet

Blockchain Innovation Program

Worksheets

Week 3 Digital Signatures

1. Digital Signatures – Craig Wright

https://craigwright.net/blog/bitcoin-blockchain-tech/digital-signatures/

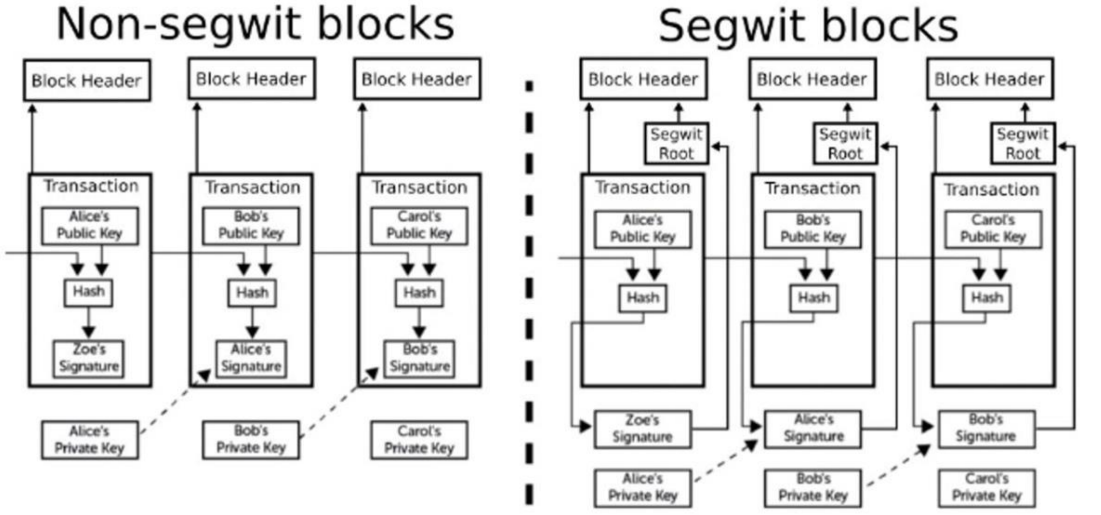
a. What is the difference between a digital signature and a digital signature algorithm?
b. Why is nonrepudiation impossible from a digital signature algorithm alone?
c. How is identity firewalled from transactions in Bitcoin?
d. Why must a contract be lawful?

2. Legitimating digital technologies in industry exchange fields: The case of digital signatures

https://www.sciencedirect.com/science/article/pii/S1471772722000057

a. Using digital signatures as a case study, what is the best mechanism to promote legitimation of novel technologies?
b. How likely will adoption be of a technology that actively flaunts the regulatory framework?

3. Non-Segwit vs Segwit

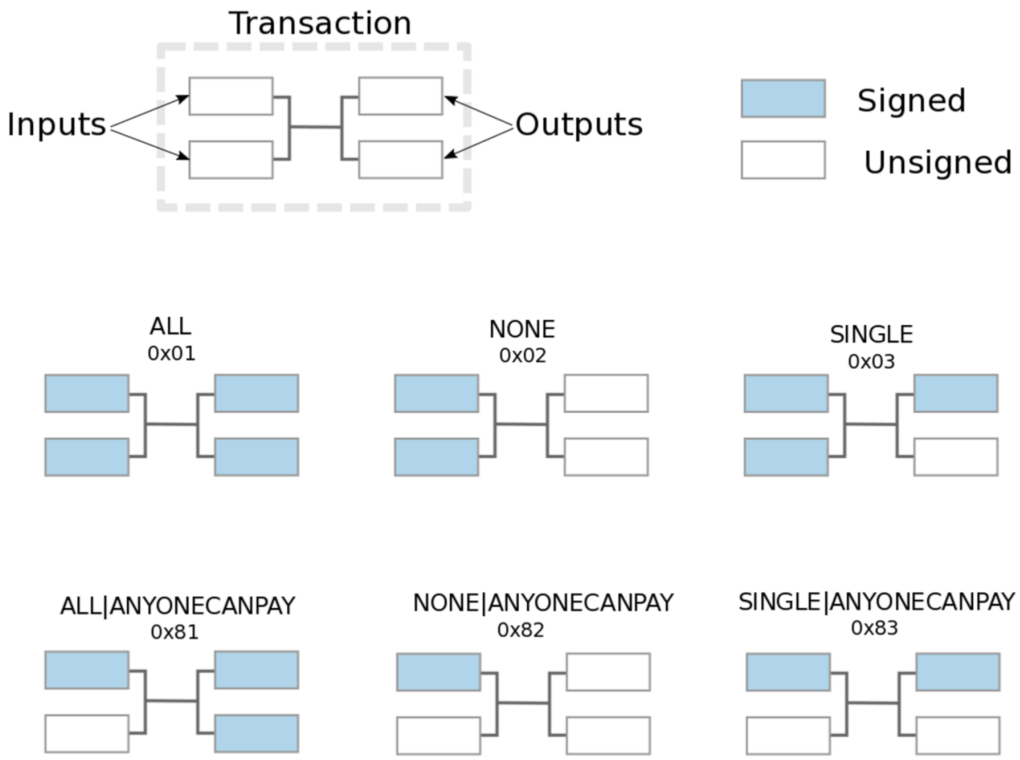


Each block header includes a cryptographically-secured reference to all of the transaction data in that block.

Each block header still includes a cryptographically-secured reference to all of the transaction data in that block, but encumbrances (public keys) are referenced separately from witnesses (signatures) so that software can use each part independently.

a. To what extent does the above imagine seem consistent with the following quote from the Introduction of the Bitcoin Whitepaper?
"We define an electronic coin as a chain of digital signatures. ***Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin****."*
b. If a technological innovation were to employ a technique of obfuscating digital signatures to enhance the capacity for anonymity, how likely would it be to be adopted by regulators?

4. **SIGHASH FLAGS**



a. How could a transaction with a SIGHASH flag that indicated that ALL ANYONECANPAY allow for novel use cases for crowd funding?
b. What ideas come to mind with the ability to selectively require signing of inputs and outputs?