ARMY CYBER INSTITUTE

COURSE SYLLABUS

Blockchain Technology

Date: March 27, 2026
Developed by:
LTC Joseph Catudal
MAJ Nicholas Harrell
CW3 Blane Richoux
LTC Karl Olson
MAJ Gabe Royal
Dr. Lubjana Beshaj
MAJ Benjamin Allison
CPT Leo Kosta
Mr. Patrick Davis
MAJ Nate Rollings
CPT Aaditya Bhatia
Approved by: COL Todd Arnold
Contact: aci.cyberops@westpoint.edu

1. Introduction

This course on blockchain technologies equips students with the technical foundation and critical perspective needed to evaluate decentralized systems. By integrating cryptography, peer-to-peer networking, and distributed consensus with real-world applications in finance, governance, and cybersecurity, the course offers a comprehensive introduction to blockchain's evolving role.

2. Learning Objectives

This course equips students with a comprehensive understanding of blockchain technologies by combining technical foundations with real-world applications and social context. Learners will explore the motivations behind decentralized trust systems, analyze cryptographic and consensus mechanisms, and compare blockchain architectures such as Bitcoin and Ethereum. Through labs, readings, and guided discussions, students will develop the skills to assess the opportunities and vulnerabilities of blockchain across domains ranging from digital currency and smart contracts to enterprise systems and government use. At the end of the course, students will be prepared to critically evaluate blockchain design decisions, understand their societal impact, and anticipate future developments in a rapidly evolving field.

By completing this course, students will be able to:

- Explain the motivations for blockchain systems compared to centralized trust models.
- Describe key blockchain primitives such as hashing, digital signatures, Merkle trees, peer-to-peer networking, and consensus algorithms.
- Compare the design and operation of Hyperledger, Bitcoin, and Ethereum.
- Deploy and manipulate basic blockchain constructs, including wallets, transactions, smart contracts, and tokens.
- Evaluate blockchain consensus mechanisms and identify trade-offs in performance, security, and decentralization.
- Analyze vulnerabilities in blockchain systems, including network and consensus threats.
- Articulate the societal and policy implications of blockchain in finance, identity, governance, and defense.
- Assess real-world blockchain applications for feasibility, scalability, and social impact.
- Track the evolution of blockchain technologies from early peer-to-peer systems to modern frameworks.
- Describe blockchain concepts effectively to technical and non-technical audiences.

3. Student Prerequisites

This course is designed for students with prior technical exposure and interest in computational systems. It assumes baseline proficiency in programming and mathematics, including familiarity with fundamental concepts such as variables, control structures, basic data structures, and algebraic reasoning. While advanced expertise is not required, students should be comfortable engaging with technical material and learning new tools independently.

The course is geared toward the freshman level of undergraduate study, with content and instruction structured to introduce foundational concepts while progressively building toward applied and analytical competence. No prior experience with blockchain technologies is assumed.

The primary target audience for this course is cyber operations practitioners and students pursuing technical disciplines related to cybersecurity, computer science, engineering, or information systems. Emphasis is placed on understanding blockchain systems from an operational, security, and analytical perspective rather than from a purely theoretical or financial standpoint.

4. Instructional Methodology and Lesson Design

Course instruction is organized around modular lessons that integrate lecture content, guided discussion, readings, and hands-on activities. All lesson materials, including slides, readings, code examples, and supporting resources, are hosted and maintained on a public GitHub repository:

[DISTRIBUTION REPO LINK]

Lessons have been prepared using Quarto slide presentations. Instruction emphasizes practical understanding of blockchain architectures, cryptographic primitives, and distributed systems through real-world examples and guided technical walkthroughs.

5. Laboratory Environment and Technical Requirements

Laboratories are a core component of the course and are designed to reinforce theoretical concepts through hands-on experimentation and applied analysis. Labs include activities such as cryptographic exercises, consensus simulations, blockchain network deployment, smart contract development, and forensic analysis.

Laboratory exercises are executed using locally run tools and delivered in one of three environments: cloud-based, locally hosted by the instructor, or run in a student virtual machine. The content can be referenced through the course GitHub repository. Students are responsible for completing labs individually unless otherwise specified.

Students are required to have:

- Personal computing workstations capable of running modern development tools (e.g., Docker, command-line interfaces, programming environments)
- Reliable Internet access to retrieve course materials, interact with online documentation, and access hosted lab instances
- The ability to install and configure required software as outlined in the course repository

All technical setup instructions, software dependencies, and lab walkthroughs are provided through the course GitHub page. Students are expected to ensure their systems meet these requirements prior to participating in lab exercises.

6. Course Structure

The curriculum emphasizes both conceptual fluency and practical experimentation. It scaffolds learning through lectures, labs, and guided analysis, preparing students not only to understand blockchain systems but also to assess their strategic, social, and ethical implications across a variety of domains.

The course consists of 36 lessons, organized into nine sections. Each section builds on the previous, moving from foundational concepts through practical implementation to real-world applications and strategic implications. The outline for the course is as follows:

a. **Introduction.** This section introduces blockchain by tracing its roots in cryptography, distributed trust, money, institutions, and peer-to-peer systems. Students examine the historical, political, economic, and philosophical motivations behind blockchain technology and develop a high-level understanding of how blockchains work before moving into the technical foundations.
b. **Cryptography Primitives.** This section establishes the core cryptographic foundations of blockchain systems, including randomness and pseudorandomness, hash functions, symmetric and asymmetric encryption, digital signatures, and Merkle trees. Students also consider cryptographic assumptions, implementation failures, and emerging challenges such as post-quantum cryptography and zero-knowledge systems.
c. **Distributed Systems Fundamentals.** This section covers the distributed-systems concepts that enable blockchain networks to operate without centralized control. Students examine peer-to-peer architecture, fault models, trust and reputation in distributed environments, distributed ledgers, and the tradeoffs between centralized, decentralized, permissionless, and permissioned designs.
d. **Consensus Mechanisms.** This section examines how blockchain networks achieve agreement on a shared state in adversarial environments. Students analyze classical consensus ideas alongside blockchain-specific approaches, with particular emphasis on Proof of Work and Proof of Stake, including their security models, incentive structures, attack surfaces, and tradeoffs in decentralization, scalability, and finality.
e. **Permissioned Chains.** This section explores blockchain systems designed for controlled membership and enterprise or institutional use. Students examine how permissioned networks differ from public blockchains in trust assumptions, governance, identity management, privacy, transaction flow, and performance. Using Hyperledger Fabric as a case study, they analyze modular architectures, endorsement logic, and practical deployment considerations.
f. **Bitcoin Framework.** This section uses Bitcoin as a case study to examine how a real-world blockchain ecosystem implements decentralized value transfer. Students study Bitcoin's origins, transaction and UTXO model, mining, peer-to-peer network structure, node behavior, scripting limitations, and major security and legal concerns.
g. **Ethereum Framework.** This section introduces Ethereum as a programmable blockchain platform built for general-purpose computation. Students examine Ethereum's architecture, governance process, EVM execution model, accounts and gas, post-Merge Proof of Stake design, smart contracts in Solidity, tokenization, digital assets, NFTs, and token-based communities.
h. **Forensics.** This section focuses on the investigative, analytical, and regulatory dimensions of blockchain ecosystems. Students examine illicit finance, transaction tracing, address clustering, attribution methods, obfuscation techniques such as mixers and tumblers, cross-chain movement, and case studies drawn from real-world criminal and enforcement activity.

i. **Applications and Synthesis.** This section examines real-world blockchain implementations and their broader societal, economic, and geopolitical implications. Topics include enterprise deployments, provenance and identity systems, CBDCs, stablecoins, state use of financial power, sanctions and global payment rails, and future technological trajectories. Students synthesize technical knowledge to evaluate feasibility, scalability, governance, and strategic impact across domains.

7. Course Schedule

This course is structured to provide 70 hours of lectures, labs, practical exercises, and discussion, suitable for accelerated instruction over a two-week period, or extended into a regular term elective course. Lesson breakdown for a regular term course consists of one lesson per course hour, adjusted for labs. Lesson breakdown for a single day of accelerated instruction to consists of four hours of lecture and discussion, two hours of lab and practical exercise work, and one hour of independent reading for students. The lesson schedule is as follows:

#	Lesson Title	Lesson Concepts, Labs, and Readings
I.	**Introduction**	
01-IN	Course Welcome and Pretest	Concepts: Course orientation
02-IN	Blockchain At A Glance	Concepts: blockchain basics, transaction lifecycle, cryptography, consensus Reading: Antonopoulos, Andreas M., and David A. Harding. Mastering Bitcoin: Programming the Open Blockchain. 3rd ed. Sebastopol, CA: O'Reilly Media, 2023. Chapter 2, "How Bitcoin Works." https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch02_overview.adoc
03-IN	Cypherpunk Ethos and Decentralized Trust	Concepts: cypherpunk movement, privacy, decentralization, digital trust Reading: Hughes, Eric. "A Cypherpunk's Manifesto." March 9, 1993. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/library/cypherpunk-manifesto/
04-IN	Money Institutions and the Case for Alternatives	Concepts: money, central banking, inflation, institutional trust Reading: Akerlof, George A. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." Quarterly Journal of Economics 84, no. 3 (1970): 488-500. https://doi.org/10.2307/1879431
L1-IN	**Social Trust Lab**	**Students perform a social game to examine the complexity**

		of maintaining social trust with untrusted parties
05-IN	Trust and Distributed Systems: Foundations for Blockchain	Concepts: distributed trust, Byzantine faults, fault tolerance, coordination Reading: Lamport, L. et al. (1982). The Byzantine Generals Problem https://nakamotoinstitute.org/static/docs/the-byzantine-generals-problem.pdf
L2-IN	**Byzantine Generals Exercise**	**Students act as systems/generals in a mutual suspicion and social trust exercise**
II.	**Cryptography Primitives**	
01-CP	Cryptography Introduction	Concepts: cryptographic security, randomness, pseudorandomness, computational hardness Reading: Boneh, Dan, and Victor Shoup. A Graduate Course in Applied Cryptography. Version 0.6. January 2023. Chapter 1. https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_6.pdf
02-CP	Hashing and Merkle Trees	Concepts: hash functions, collision resistance, Merkle trees, data integrity Reading: Chapter 7, Barak, Boaz (2021). An intensive introduction to cryptography. https://intensecrypto.org/public/index.html
03-CP	Symmetric Encryption	Concepts: symmetric encryption, block ciphers, stream ciphers, authenticated encryption Reading: Chapter 3, Barak, Boaz (2021). An intensive introduction to cryptography. https://intensecrypto.org/public/index.html
04-CP	Asymmetric Encryption and Digital Signatures	Concepts: public-key cryptography, key exchange, RSA and ECC, digital signatures Reading: Diffie, Whitfield, and Martin Hellman. "New Directions in Cryptography." IEEE Transactions on Information Theory 22, no. 6 (1976): 644-654. https://doi.org/10.1109/TIT.1976.1055638
L1-CP	**Hashing and Cryptography Lab**	**Students conduct hashing operations and review implementations of symmetric and asymmetric cryptography**
05-CP	Cryptographic Assumptions and Challenges	Concepts: post-quantum cryptography, zero-knowledge proofs, homomorphic encryption, cryptographic failures Reading: Boneh, Dan, and Victor Shoup. A Graduate Course in Applied Cryptography. Version 0.6. January 2023. Chapter 17. https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_6

		.pdf
III.	**Distributed Systems Fundamentals**	
01-DS	Distributed Systems	Concepts: distributed systems, client-server vs P2P, network fallacies, failure models Reading: Deutsch, L. Peter, James Gosling, Mike Burrows, and others. "The Eight Fallacies of Distributed Computing." n.d. PDF. https://arnon.me/wp-content/uploads/Files/fallacies.pdf
02-DS	P2P Design	Concepts: overlay networks, distributed hash tables, routing, churn Reading: Stoica, Ion, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan. "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications." ACM SIGCOMM Computer Communication Review 31, no. 4 (2001): 149-160. https://doi.org/10.1145/964723.383071
03-DS	Trust and P2P	Concepts: reputation systems, social trust, Sybil attacks, collusion Reading: Kamvar, S. et al. (2003). The EigenTrust Algorithm for Reputation Management in P2P Networks https://dl.acm.org/doi/10.1145/775152.775242
L1-DS	**P2P Lab**	**Explores models of distributed systems and several threat scenarios in system trust relationships**
04-DS	Distributed Ledgers	Concepts: distributed ledgers, permissionless vs permissioned, immutability, governance Reading: UK Government Office for Science. Distributed Ledger Technology: Beyond Block Chain. London: Government Office for Science, 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
IV.	**Consensus Mechanisms**	
01-CM	Consensus in Distributed Systems and Blockchains	Concepts: consensus properties, safety and liveness, BFT, Nakamoto consensus Reading: Cachin, Christian, and Marko Vukolic. "Blockchain Consensus Protocols in the Wild." In 31st International Symposium on Distributed Computing (DISC 2017). 2017. https://cybersecurity.seas.wustl.edu/ning/paper/consensus19.pdf
02-CM	Proof of Work and Security	Concepts: proof of work, mining incentives, difficulty adjustment, chain security Reading: Antonopoulos, Andreas M., and David A. Harding.

		Mastering Bitcoin: Programming the Open Blockchain. 3rd ed. Sebastopol, CA: O'Reilly Media, 2023. Chapter 12, "Mining and Consensus." https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch12_mining.adoc
03-CM	Proof of Stake	Concepts: proof of stake, validator selection, slashing, finality Reading: Wang, Xuechao, Govinda Kamath, Vivek Bagaria, Sreeram Kannan, Sewoong Oh, David Tse, and Pramod Viswanath. "Proof-of-Stake Longest Chain Protocols Revisited." CoRR abs/1910.02218 (2019). https://doi.org/10.48550/arXiv.1910.02218
L1-CM	**Consensus Lab**	**Students observe and manipulate adjustable simulations for PoW and PoS consensus mechanisms**
V.	**Permissioned Chains**	
01-PC	Permissioned Distributed Ledgers	Concepts: permissioned blockchain, identity management, deterministic finality, governance controls Reading: Androulaki, Elli, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, and others. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains." In Proceedings of the Thirteenth EuroSys Conference, 1-15. New York: ACM, 2018. https://doi.org/10.1145/3190508.3190538
02-PC	Hyperledger Fabric	Concepts: Hyperledger Fabric, endorsement policies, MSP and CA, channels Reading: Hyperledger Foundation. Hyperledger Fabric Documentation. Release 2.5. 2024. https://hyperledger-fabric.readthedocs.io/en/release-2.5/
L1-PC	**Hyperledger Lab**	**Students create, deploy, and manipulate a permissioned blockchain using Hyperledger Fabric**
VI.	**Bitcoin Framework**	
01-BF	Bitcoin Origins Mechanics and Roadmap	Concepts: Bitcoin origins, double spending, proof of work, decentralized money Reading: Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System https://cdn.nakamotoinstitute.org/docs/bitcoin.pdf
02-BF	Bitcoin Transactions and Mining	Concepts: UTXO model, wallets and addresses, transaction flow, block mining Reading: Antonopoulos, Andreas M., and David A. Harding. Mastering Bitcoin: Programming the Open Blockchain. 3rd ed. Sebastopol, CA: O'Reilly Media, 2023. Chapter 6,

		"Transactions." https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06_transactions.adoc
03-BF	Bitcoin Nodes and Network	Concepts: Bitcoin nodes, peer discovery, block propagation, Bitcoin Script Reading: Antonopoulos, Andreas M., and David A. Harding. Mastering Bitcoin: Programming the Open Blockchain. 3rd ed. Sebastopol, CA: O'Reilly Media, 2023. Chapter 10, "The Bitcoin Network." https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch10_network.adoc
04-BF	Bitcoin Security and Legal Concerns	Concepts: routing attacks, selfish mining, deanonymization, KYC/AML Reading: Apostolaki, Maria, Aviv Zohar, and Laurent Vanbever. "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies." In 2017 IEEE Symposium on Security and Privacy (SP), 375-392. Los Alamitos, CA: IEEE Computer Society, 2017. https://doi.org/10.1109/SP.2017.29
L1-BF	**Bitcoin Lab**	**Students create wallets, mine blocks, generate transactions, and explore those transactions on the regtest network using command line tools and custom scripts**
VII.	**Ethereum Framework**	
01-EF	Ethereum Introduction	Concepts: Ethereum architecture, EVM, gas, governance Reading: Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf
02-EF	Ethereum Mining PoS and Security	Concepts: Ethereum PoS, validators, randomness, Gasper Reading: Asgaonkar, Aditya, et al. "Ethereum's Proof-of-Stake Consensus Layer." CoRR abs/2310.01028 (2023). https://doi.org/10.48550/arXiv.2310.01028
03-EF	Ethereum Network	Concepts: Ethereum transactions, mempool, clients and nodes, MEV Reading: Antonopoulos, Andreas M., Gavin Wood, Carlo Parisi, Alessandro Mazza, and Niccolo Pozzolini. Mastering Ethereum. 2nd ed. Sebastopol, CA: O'Reilly Media, 2026. Chapter 3, "Ethereum Nodes." https://masteringethereum.xyz/chapter_3.html
04-EF	Smart Contracts	Concepts: smart contracts, Solidity, contract deployment, EVM execution Reading: Antonopoulos, Andreas M., Gavin Wood, Carlo

		Parisi, Alessandro Mazza, and Niccolo Pozzolini. Mastering Ethereum. 2nd ed. Sebastopol, CA: O'Reilly Media, 2026. Chapter 7, "Smart Contracts and Solidity." https://masteringethereum.xyz/chapter_7.html
L1-EF	**Ethereum Lab**	**Students conduct operations on EVM and develop their own smart contracts using Solidity**
06-EF	Digital Assets Tokenization and NFTs	Concepts: tokenization, fungibility, NFTs, metadata Reading: Ethereum.org (2025). ERC-20 Token Standard https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
07-EF	Token-Based Communities and NFTs in Practice	Concepts: token communities, token gating, minting, on-chain vs off-chain value Reading: Ohlhaver, Puja, E. Glen Weyl, and Vitalik Buterin. "Decentralized Society: Finding Web3's Soul." SSRN Electronic Journal (2022). https://doi.org/10.2139/ssrn.4105763
L2-EF	**Token Lab**	**Students develop, mint, and trade fungible and non-fungible tokens**
VIII.	**Forensics**	
01-FO	Illicit Finance Forensics and Regulation	Concepts: illicit finance, regulation, blockchain tracing, enforcement case studies Reading: Sykes, J. et al. (2019). Virtual Currencies and Money Laundering https://www.congress.gov/crs_external_products/R/PDF/R45664/R45664.2.pdf
02-FO	Blockchain Forensics	Concepts: address clustering, mixers and tumblers, tracing heuristics, cross-chain laundering Reading: Atlam, Hany F., Ndifon Ekuri, Muhammad Ajmal Azad, and Harjinder Singh Lallie. "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions." Electronics 13, no. 17 (2024): 3568. https://doi.org/10.3390/electronics13173568
L1-FO	**Forensics Labs**	**Examines mixers and coinjoin operations, and provides several forensic scenarios for students to investigate**
IX.	**Applications and Synthesis**	
01-AS	Blockchain in the Real World	Concepts: real-world adoption, custody and wallets, oracles, interoperability Reading: Congressional Research Service. Blockchain: Novel Provenance Applications. CRS Report R47064. Washington,

		DC: Congressional Research Service, April 8, 2022. https://www.congress.gov/crs-product/R47064
02-AS	CBDCs and Stablecoins	Concepts: CBDCs, stablecoins, digital money, payment infrastructure Reading: Bank for International Settlements. "The Future Monetary System." In Annual Economic Report 2022, chap. 3. Basel: Bank for International Settlements, 2022. https://www.bis.org/publ/arpdf/ar2022e3.htm
03-AS	Blockchain in Geopolitical Competition	Concepts: sanctions, state power, cryptocurrency policy, geopolitical competition Reading: TRM Labs. Hidden Signals on the Blockchain: Why National Security Needs Blockchain Intelligence. March 10, 2026. https://www.trmlabs.com/reports-and-whitepapers/hidden-signals-on-the-blockchain
04-AS	Technical Concepts Review	Summary review of course technical material and its use in blockchain applications
05-AS	Future Trajectories and Synthesis	Concepts: future scenarios, decentralization, AI and blockchain, strategic outlook Reading: Buterin, Vitalik. "The Meaning of Decentralization." Medium, February 6, 2017. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274