SYLLABUS
Queens College/CUNY

Math 290.3 Introduction to the Mathematics of Blockchain. 3 hr.; 3 cr.

INSTRUCTOR INFORMATION: Kenneth Goodman, office hours will be after class on Tuesday from 745pm – 830pm. If that time does not work, please email me at least one week in advance to set up an appointment. Please don't wait until the class before the test; I may not be able to accommodate you if I don't have prior notice. Please email me with any questions you may have and I will respond as soon as I can.

A. COURSE DESCRIPTION

Prereq.: C- or better in MATH 241 or permission of the department.

Presents the basic concepts of information theory, hashing functions, and puzzle-friendly hashing functions.

The class explores: partial hash-preimage puzzles, merkle trees, trapdoor functions, multiplicative congruence classes, zero-knowledge proofs and new research in blockchain and cryptocurrencies.

This course is aligned with the Core Values of the Education Unit of promoting ***Equity***, ***Excellence***, and ***Ethics*** in urban schools and communities. More specifically, the Education Unit is committed to preparing teachers and other school professionals who: a) build inclusive communities that nurture and challenge all learners; b) demonstrate professionalism, scholarship, efficacy, evidence-based practice and reflection; and c) value diversity, democracy, and social justice.

B. COURSE LEARNING GOALS & OBJECTIVES

1. Students should be able to talk knowledgeably about blockchain and cryptocurrencies
2. Students should have the ability to pass the "Certified Bitcoin Professional" exam
3. Students should have the knowledge and skillset to explore other topics in crypto-assets, not just blockchain or currencies.

C. TEXTBOOKS AND RESOURCES

Entropy Measures and Unconditional Security in Cryptography
Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
The Higher Arithmetic (optional)
http://bitcoinbook.cs.princeton.edu/
http://chimera.labs.oreilly.com/books/1234000001802/index.html

D. COURSE TOPICS/UNITS/READINGS AND DATES WEEKLY TENTATIVE SCHEDULE

Schedule I'll be looking at: http://www2.cuny.edu/academics/academic-calendars/

A * means you should complete all the readings in that section.

Week	Topic	Readings/Videos	Notes
1/28	What is a blockchain? Why are we studying this? Probability Review Poisson Process Discrete Probability	1* 10* 2.2*	First class - 2/2 last day to drop for 75% refund

Week	Topic	Readings/Videos	Notes
2/4	Hashing Functions Collision-resistance Hiding Puzzle Friendliness Progress Free Merkle Trees	2.1*	2/9 - last day to drop for 50% refund
2/11	Proof Of What? Proof Of Work Proof Of Stake Proof Of Storage Proof Of Burn	5*	2/16 - last day for 25% refund 2/17 - first day to withdraw from a course with a grade of W
2/18	Public-Private Key Cryptography Intro	6.1 6.4	2/20 - Classes follow a Monday schedule, no class
2/25	Multiplicative Cyclic Groups Diffie-Hellman Key Exchange Discrete Logarithm Problem Trapdoor and one way Functions	6.1-6.5*	
3/4	Elliptic Curves Addresses	6.6	
3/11	Distributed Ledgers Analysis Of Nakamoto's Double Spend Attack	1.1 7.4	Midterm Proposal Due
3/18	Introduction to Anonymity CoinJoin Zerocoin Ring CT ZkSnarks/ZkStarks Dandelion	12.1 12.8-12.9* 11.11-11.13* 11.16-11.17*	
3/25	Introduction to scaling: Lightning Network Block Increases Block Time Sharding L2 and L3 Solutions Sidechains/Drivechains SegWit	4*	Midterm Paper Due
4/1	Spring Recess	Spring Recess	Spring Recess
4/8	Introduction to bootstrapping coins: Difficulty Adjustments Inflation Proof of …..?	5*, 9*	
4/15	Attacks: Forks Double Spend DoS Sybil Replay attacks	3*, 7*	4/16 - last day to withdraw from a course with a grade of W

Week	Topic	Readings/Videos	Notes
4/22	Other Cryptographically Secure Data Structures - Dags, Parallel Chains	11*	Final Paper Proposal Due - 4/26
4/29	Group Project Discussion		Draft Meetings
5/6	Group Project Discussion		
5/13	Review		Last class this week
5/20	NA		Final Paper Due - 5/24

E. ASSIGNMENTS, DUE DATES AND GRADING PLAN

Percentage	Description	Due Date
10%	Reading Responses	NA
2.5%	Midterm Paper Proposal	Midnight EST 3/15/2018
27.5%	Midterm Paper	Midnight EST 3/31/2018
10%	Questions/Participation To Other Final Presentations	
5%	Final Paper Proposal	Midnight EST 4/26/2018
45%	Final Presentation/Paper	Midnight EST 5/24/2018

Reading Responses (10 - 14%):

Reading Responses will be worth 1 point per week. It must be a minimum of 150 words and no longer than 300 words. There are 12 weeks of reading, you may skip 2 and still get full points. If you do all 12, you will get a bonus of 2 extra points, so 14 total. You may respond to someone else or talk about a completely different reading. Feeling up to it, bring in a new paper/dev-email/video/reddit-post and respond to that. All responses will be done on reddit, see: https://www.reddit.com/r/QCMath2903/ after I add the class.

Extra Credit:

There are always extra credit opportunities regarding reading assignments if you come speak to me.

Midterm Proposal (5%):

Propose a topic that you will write upon. Outlining your paper here would help yourself write the paper as well as give me a place to give you feedback.

Midterm Paper (25%):

The midterm paper must be more than 3 pages, not including sources. Single spaced, 1 inch margins all around. 12 Times New Roman font. I won't measure, but it'll be obvious if you're trying to fill up space versus put actual material there.

The paper must be an in-depth explanation into a topic we **have** covered in class up to this point. It must be related to cryptographically secured data structures.

There must be at least one source that comes from a published paper.

Final Proposal (5%):

You may choose the weight for your final presentation and paper. The weights for both must add up to 45 points. Each must be between 10 and 35 points. In your proposal, you must send me your weights. For example, a great public speaker might be: 35 points for the presentation and 10 for the paper. Someone less confident in public speaking, may choose the reverse. You will have to explain why you have put more weight on either. Ie: A great presentation worth 35 points might have handouts, probing questions, and classroom interaction. A great paper worth 35 points might be more detailed, include graphs, code, citations, unique, etc.

Propose a topic that you will write upon. Outlining your paper and making an agenda for the presentation here would help yourself as well as give me a place to give you feedback.

Final Paper (10-35%):

The final paper must be more than 2 pages (4.5 if you choose 35% for the paper), not including sources. Single spaced, 1 inch margins all around. 12 Times New Roman font. I won't measure, but it'll be obvious if you're trying to fill up space versus put actual material there.

The paper must be an in-depth explanation into a topic we **haven't** covered in class. This will be an opportunity for you to do self-paced guided learning. It must be related to cryptographically secured data structures.

There must be at least one source that comes from a published paper.

Letter Grade	Percentage	Performance
A+	97-100%	Above Excellent Work
A	93-96%	Excellent Work
A-	90-92%	Nearly Excellent Work
B+	87-89%	Very Good Work
B	83-86%	Good Work
B-	80-82%	Mostly Good Work
C+	77-79%	Above Average Work
C	73-76%	Average Work
C-	70-72%	Mostly Average Work
D+	67-69%	Below Average Work
D	60-66%	Poor Work

Letter Grade	Percentage	Performance
F	0-59%	Failing Work

F. REASONABLE ACCOMMODATIONS FOR CANDIDATES WITH DISABILITIES
Candidates with disabilities needing academic accommodation should: 1) register with and provide documentation to the Special Services Office, Kiely 171; 2) bring a letter to me indicating the need for accommodation and what type. This should be done during the first two weeks of class. For more information about services available to Queens College candidates, contact: Special Service Office; 171 Kiely Hall; 718-997-5870 (8:00 a.m. to 5:00 p.m.).

G. CUNY POLICY ON ACADEMIC INTEGRITY
The Policy on Academic Integrity, as adopted by the Board is available to all candidates. Academic Dishonesty is prohibited in The City University of New York and is punishable by penalties, including failing grades, suspension, and expulsion. This policy and others related to candidates' issues are available to you at: http://qcpages.qc.cuny.edu/provost/Policies/index.html.

H. MY POLICY ON ACADEMIC INTEGRITY
If caught cheating or plagiarizing, you will get a zero on the assignment and will not have an opportunity to make it up; you will be reported to the appropriate committee.

I. Readings:

1. Blockchain/Bitcoin Basics:
    1. Bitcoin White Paper With Notation
    2. Video: An intuitive explanation to why and how blockchain was invented 3b1b - great overview
    3. Text: WTF is the blockchain
    4. Bitcoin's Academic Pedigree
    5. Short and to the point graphical explanation of bitcoin process to add a block
2. Hashing & Probability:
    1. Hashing:
        1. Video: Computerphile - SHA
        2. Video: How Secure Is Sha256
        3. Hash online
        4. https://en.wikipedia.org/wiki/Merkle_tree
    2. Poisson Process:
        1. Poisson Point Process
        2. Video: Khan Academy Poisson Process
        3. Poisson Limit Theorem
3. Forks
    1. Chain Fork Explained - Double Spending
    2. Forkology
    3. Bitcoin Fork (UASF/UAHF) - ulterior motives?
    4. Why SPV wallets are dangerous for forks
4. Scaling Bitcoin
    1. Lighting Network
        1. Mathematical Proof That LN is not a cheap decentralized solution for scaling
    2. Atomic Swaps on the LN
    3. Understanding the LN
    4. SegWit:
        1. Main Advantages of SegWit
        2. What is Segwit

        1. Slides
    3. Segwit2x or not
    5. Accelerating Bitcoin's Trasaction Processing
    6. Graphene: Block Propagation Using Set Reconciliation (Proposal as of Aug 2017)
5. Proof Of What?
    1. Proof Of Work:
    2. Proof Of Stake:
        1. PoS Primer
        2. What Proof Of Stake (POS) is and why it matters
    3. Proof Of Burn:
    4. Proof Of Storage/Capacity:
6. Public-Private Key:
    1. Ellipitc Curves 101 - Public - Private Key
    2. Digital Signatures Basic Example
    3. Video: Computerphile on ECC
    4. Video: Diffie-Hellman
    5. Video: Lecture on ECC
    6. Mastering Bitcoin - Ch4
7. Bugs/Attacks:
    1. Bancor front runner bug
    2. Zcoin zerocoin bug
    3. Parity Hack explained
    4. An Explanation of Nakamoto's Analysis of Double-spend Attacks
8. ICOs:
    1. ICOs and economics of lemon markets
9. Bootstrapping:
    1. Emergency Difficulty Adjustment (Bitcoin Cash)
    2. Gravity Wells
    3. MIDAS
    4. Dark Gravity Wave (Used By Dash)
    5. DigiShield
    6. Zcash Retargeting Specifications
    7. Analysis of different params
10. Misc:
    1. How Money Moves Around The World Now
11. Dags and other cryptographically secure data structures:
    1. IOTA Whitepaper
    2. RaiBlocks WhitePaper
    3. Byteball Whitepaper
12. Anonymity:
    1. Zerocoin Whitepaper
    2. Zero Knowledge
    3. Zerocoin Video Primer
    4. Zcash FAQs: Zero-Knowledge
    5. Zcoin zerocoin bug
    6. Christina Garman - Zerocoin/ZCash and more
    7. zk-snarks under the hood for ETH
        1. precompiling zk-snarks proofs in ETH
    8. Great overview of zk-snarks
    9. Ring Signature Paper
        1. Monero Ring Signature Paper
    10. Exploration of Group and Ring Signatures
    11. Dandelion: Adding some anonymity to Bitcoin (proposal as of Aug 2017)
    12. Sybil-Resistant Mixing
    13. Comparison of different anonymity protocols
    14. A Fistful of Bitcoins: Characterizing Payments Among Men With No Names (heuristic address clustering)
    15. Confidential Transactions:

1. Original Proposal Thread (Adam Black)
    1. Homomorphic Encryption (Wiki)
2. Simple explanation of confidential transactions (CT)
3. CT and CoinJoin
4. Confidential Assets (extension of CT?)
5. Bulletproofs - efficient zero knowledge. CT Optimization
6. Confidential Assets

16. Coinjoin holes (Dash)
17. Monero Deanonymization