Indian Institute of Technology Kanpur

Syllabus

Course Title: Blockchain Technology and Applications

Course No: CS731A

Credits: 3-0-0-0- [9]

Prerequisite: Expertise in programming, basic knowledge of computer security, cryptography, networking, concurrent or parallel programming would help a student to understand the topics.

Co-requisite: CS628 [Computer Systems Security] (Not necessary but preferable)

Who can take the course: Ph.D., Masters, 3rd and 4th year UG Students

Instructor:

Sandeep Kumar Shukla,
Professor,
Department of Computer Science and Engineering
sandeeps@cse.iitk.ac.in
Room: RM 508

Course Rationale:

Blockchain is an emerging technology platform for developing decentralized applications and data storage, over and beyond its role as the technology underlying the cryptocurrencies. The basic tenet of this platform is that it allows one to create a distributed and replicated ledger of events, transactions, and data generated through various IT processes with strong cryptographic guarantees of tamper resistance, immutability, and verifiability. Public blockchain platforms allow us to guarantee these properties with overwhelming probabilities even when untrusted users are participants of distributed applications with ability to transact on the platform. Even though, blockchain technology has become popularly known because of its use in the implementation of Cryptocurrencies such as BitCoin, Ethereum, etc., the technology itself holds much more promise in various areas such as time stamping, logging of critical events in a system, recording of transactions, trustworthy e-governance etc. Many researchers are working on many such use cases such as decentralized public key infrastructure, self-sovereign identity management, registry maintenance, health record management, decentralized authentication, decentralized DNS, etc. Also, corporations such as IBM and Microsoft are developing their own applications in diverse fields such as the Internet of Things (IoT), etc., even enabling blockchain platforms on the cloud.

Considering the need to disseminate the emerging concepts for students, we decided to prepare a new course on blockchain technology platforms and applications.

The students will be exposed to the following topics:

1. Basic Cryptographic primitives used in Blockchain – Secure, Collison-resistant hash functions, digital signature, public key cryptosystems, zero-knowledge proof systems
2. Basic Distributed System concepts – distributed consensus and atomic broadcast, Byzantine fault-tolerant consensus methods
3. Basic Blockchain (Blockchain 1.0) – concepts germane to Bitcoin and contemporary proof-of-work based consensus mechanisms, operations of Bitcoin blockchain, crypto-currency as application of blockchain technology
4. Blockchain 2.0 – Blockchains with smart contracts and Turing complete blockchain scripting – issues of correctness and verifiability, Ethereum platform and its smart contract mechanism
5. Blockchain 3.0 – Plug-and-play mechanisms for consensus and smart contract evaluation engines, Hyperledger fabric platform
6. Beyond Cryptocurrency – applications of blockchain in cyber security, integrity of information, E-Governance and other contract enforcement mechanisms
7. Limitations of blockchain as a technology, and myths vs. reality of blockchain technology
8. Research directions in Blockchain technology

The course will be ***very heavy on projects*** and require ability to quickly configure a new development platform and use it, develop applications, and move to a new one. At least three blockchain platforms will be used in projects in the course. The course will consist of instructor presentations, demonstrations, and hands-on projects.

Module	**Topic**	**No. of 1 hour Lectures**
Introduction	Need for Distributed Record Keeping Modeling faults and adversaries Byzantine Generals problem Consensus algorithms and their scalability problems Why Nakamoto Came up with Blockchain based cryptocurrency? Technologies Borrowed in Blockchain – hash pointers, consensus, byzantine fault-tolerant distributed computing, digital cash etc.	**3**
Basic Distributed Computing	Atomic Broadcast, Consensus, Byzantine Models of fault tolerance	**4**

Basic Crypto primitives	Hash functions, Puzzle friendly Hash, Collison resistant hash, digital signatures, public key crypto, verifiable random functions, Zero-knowledge systems	**4**
Blockchain 1.0	Bitcoin blockchain, the challenges, and solutions, proof of work, Proof of stake, alternatives to Bitcoin consensus, Bitcoin scripting language and their use	**5**
Blockchain 2.0	Ethereum and Smart Contracts, The Turing Completeness of Smart Contract Languages and verification challenges, Using smart contracts to enforce legal contracts, comparing Bitcoin scripting vs. Ethereum Smart Contracts	**8**
Blockchain 3.0	Hyperledger fabric, the plug and play platform and mechanisms in permissioned blockchain	**8**
Privacy, Security issues in Blockchain	Pseudo-anonymity vs. anonymity, Zcash and Zk-SNARKS for anonymity preservation, attacks on Blockchains – such as Sybil attacks, selfish mining, 51% attacks - -advent of algorand, and Sharding based consensus algorithms to prevent these	**8**
Total Lecture hours		**40 hours**

Text:

There is no textbook for such a course yet. One in preparation from the instructor and his colleagues is still in writing stage but some sample chapters will be used.

Reference Books:

1. Draft version of "S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, 'Blockchain Technology: Cryptocurrency and Applications', Oxford University Press, 2019.
2. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.

There will be other resources put on the web by the instructor.

- Lecture notes, assignments, supplemental readings, and other resources will be provided via the course website
- The course will consist of 3 hours of lectures per week, projects and homework, and possibly a course project.

- **Grading**

Semester grades will be based on the following weights:

Attendance & In-Class Exercises	10%	(including pop quizzes)
Projects & Assignments	70%	(10% each for 7 assignments and projects)
Midterm Exam	10%	
Final Exam	10%	

Semester grades will be determined after all work is completed and graded. Point ranges for letter grades will be based on a several factors, including absolute and relative performance. Letter grades will not be based on a curve or point range.

Unless otherwise stated on the class **all graded assignments must be submitted by 11:55 pm on the specified due date via course site on canvas.** There will be a 10% penalty for each 24 hour delay in submitting an assignment.

If you feel that an error is made in grading an assignment or an exam, you must present a written appeal within one week after the assignment or exam is returned to you. Verbal appeals are not allowed, and grades will not be changed after the one week period. Your appeal should be specific. Submit all appeals to the instructor.