MAS.S65 - Blockchain Technologies: Decentralize all the Things

Instructors: Guy Zyskind, Chelsea Barabas, Anders Brownworth
TA/Mentors: TBD
Faculty Director: Sandy Pentland

Course Description

With more than $800 million in venture capital invested in digital currency-related startups over the last several years, bitcoin and other cryptocurrencies have become a fast-growing emerging technology. Some people claim that a decentralized public ledger, like the blockchain, will significantly improve our ability to make and receive payments, increase transparency in government and financial markets, and increase the interoperability of our personal data like medical or educational records while also increasing our ability to control who has access to them. Others argue that digital currencies like Bitcoin are fundamentally flawed and will never achieve the widespread adoption that more centralized infrastructures currently enjoy.

The goal of this course is to help you make your own decision by teaching you how to work with digital currencies like bitcoin and give you an understanding of how to use this technical skill to impact the economics, privacy, and interoperability that are driving the adoption of bitcoin and other cryptocurrencies.

In this project-based class, students will develop a foundational understanding of how the blockchain works by engaging with leading thinkers in this space while working on their own ideas for using the blockchain as a foundational tool for addressing real-world problems.

By the end of the class, students will have a firm grasp on the scope of real-world applications that can be built on top of the blockchain, as well as the challenges and questions that still need to be resolved in order for these use cases to move from the realm of science fiction to reality.

Course Themes

Blockchain fundamentals - the technology behind Bitcoin and other digital currencies.
Cross-disciplinary digital currency research themes - i.e. scalability, privacy, and identity.
Developing applications on the blockchain - key considerations for designing applications that survive "in the wild"

Course Pre-requisites

This class provides the technical and scientific foundations underlying digital currencies. It is meant to give researchers the tools necessary to begin developing on the blockchain. Students who are familiar with programming and probability theory will be best-suited to succeed. This is a graduate course offering.

Course Format

This class will be focused on developing a foundational technical understanding of the blockchain, which will prepare students to think comprehensively about integrating the blockchain.

- First half of semester will be a technical deep-dive, in which we outline the tools and processes necessary to develop applications. We will assign a single problem set given in the second week of class and due halfway through the class. It covers the technical foundations (cryptographic basics, distributed consensus, operating bitcoin internals, developing a MockCoin). This ensures all students understand the technology before developing their project.
- Second half of semester will be focused on developing student projects and exploring research questions with leading experts in the field. Students will form teams of 3 to conceive of projects that are centered around addressing one specific technical "pain point" that we face in developing real-world applications on the blockchain (i.e. usability, offline transactions, blockchain forensics, etc.).
    - Example final projects:
    - Project teams are 3-4 people

Grading:

20% class participation
30% homework assignments, psets
50% final project *(20% project proposal presentation/critique, 30% final presentation)*

Week	Topic(s)	In-Class Activity/Assignments
9/9 Week 1	*Overview of the technology.* Getting people excited. • Basic technical description of blockchain	Sign up for class activity. **Assignment:** Join IRC and dev mailing list.

	technology and digital currencies • History and achievements • List of interesting projects (bite-sized) • A very simplified explanation of how it works (leading to the next more technical lectures)	
9/16 Week 2	Crypto 101 : • Cryptographic hashes ◦ Definition ◦ SHA256 / DSHA256 / SHA3 • Encryption (as opposed to hashing) • Digital signatures ◦ Definition ◦ History: RSA, DSA • Elliptic Curve Cryptography ◦ ECDSA • Cryptographic puzzles • Hash pointers ◦ Hash chains ◦ Merkle trees • Tie it all together -- how all these things fit into bitcoin (precursor to next lecture)	**Reading:** *Video from BlackHat* - Bitcoin: A Peer-to-Peer Electronic Cash System **Discussion:** Bitcoin relies on some of the â€œmost secureâ€ technologies/cryptographic methods available today, but whatâ€™s the time horizon we should expect for these methods to remain secure? On what assumptions are crypto-systems like bitcoin built upon, and what may cause them to break in the future? **Homework:** PSET 1 ASSIGNED
9/23 Week 3	*How Bitcoin works (achieving decentralization)* • 'Centralized' bitcoin (i.e., introducing bitcoin with a centralized ledger)	**Reading:** Michael Nielsenâ€™s How the Bitcoin Protocol Actually Works Read thru BIP guidelines BIP -- 70, 37 **Discussion:** **No discussion this week.**

	• The blockchain structure
	  ◦ Transactions
	  ◦ Blocks
	• Distributed consensus
	  ◦ Byzantine Agreement (informally)
	  ◦ Proof-of-Work
	  ◦ Incentives
	• How a multidisciplinary approach succeeded where CS theory alone failed. What can we learn from it. How can we jointly model multiple disciplines?
	• The P2P network
	  ◦ Full nodes
	  ◦ Miners
	  ◦ SPV nodes (original proposal)
	  ◦ SPV nodes today (BIP 37 + Bloom Filters)
	• Bitcoin scripting
	  ◦ Stack Language
	  ◦ P2PKH, Multi-Sig (Tree-sigs as well?), P2SH
	  ◦ OP_RETURN
		Homework:
		PSET 1 DUE PSET 2 ASSIGNED

9/30 Week 4	*Bitcoin ecosystem*
	
	• Hard/soft forks
	• BIP38 and PBKDFs
	• Wallets
	  ◦ Hot/cold
	  ◦ HD wallets
		Reading:
		BIP38
		
		Moore, Tyler, and Nicolas Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk.

	◦ Online (e.g., coinbase) ◦ Colored • Exchanges • Mining pools and centralization	Bonneau, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. **Discussion:** Bitcoin is described as a decentralized payment system -- but is it really decentralized? What are the components of bitcoin's system that push it towards greater centralization over time? Why? **Homework:** PSET 2
Week 5	*Moving beyond Bitcoin - Decentralize all things!* • Different ways of interacting with bitcoin ecosystem for different application scenarios (altcoins, layers on top blockchain, sidechains, new blockchain, sidechains, private blockchains) • Altcoins • Different consensus mechanisms • Better programmability for broader use cases ◦ Smart contracts, Ethereum • Sidechains • Data layers - using blockchain as â€œanchorâ€ and Factom	**Reading:** Andrew Poelstra - Treatise on Altcoins **Discussion:** Do we agree with the popular idea that â€œitâ€™s all about the blockchain, not bitcoinâ€? How do we foresee new features getting successfully integrated into the digital currency ecosystem? Are alternatives like Ethereum a threat or complementary to Bitcoin? How do we foresee this ecosystem evolving moving forward? **Homework:** PSET 2 due, assign PSET 3
Week 6	**Applications overview:** 3 30-minute student-led	**Reading:** No mandatory reading this week.

	presentations (in pairs) on Ethereum, Stellar Consensus, Stellar 3 10-15 minute presentations on one of the following applications: • Prediction Markets • Proof-of-existence (IP, contracts, etc â€¦); MIT Certificates • Promissory • File Storage • Proof-of-X • etc â€¦	**Discussion:** Students cover different key projects more in-depth (Ethereum, Sidechains, Stellar) **Homework:** PSET 3
Week 7	Blockchain application case studies - bring in 2-3 speakers from partner orgs, have them break down a problem space theyâ€™re working on that they think might have applications to blockchain. Technical roadblocks/challenges to it being adopted/integrated into current systems/markets	**Reading** Background read to be provided by partner orgs **Discussion** Whole class is a discussion! No moderator needed. **Homework:** PSET 3 due Review project proposal guideline
Week 8	*Digital Currency's Challenges: Scalability* In depth look into the major roadblocks and the major issues for the future of blockchain tech. • Scalability concern - risks and considerations • Proposed solutions: ◦ blocksize - BIP 100, BIP	**Reading:** BIP100, BIP101 Why is Bitcoin forking How the Bitcoin Experiment Might Fail Lightning Network White Paper **Discussion:** No extra discussion **Homework:** Report teams Write project proposal

	101, Bitcoin XT ◦ lightning networks • How to make technical decisions that address the needs of government, consumer, private sector ◦ Economic models for miners and wallets -- trade-offs in how different scaling solutions will impact the decentralized nature of network, costs to user, etc.	
Week 9	*Digital Currency's Challenges: Usability* In depth look into the major roadblocks and the major issues for the future of blockchain tech. • Developing for the developing world ◦ Offline transactions: Accessing the blockchain in places w/low internet connectivity ◦ On/off ramping in cash-driven economies	**Discussion:** Student project proposal presentations

	(fiat-digital-fiatl)	
Week 10	*Digital Currency Challenges: Privacy/Identity/Research* • Enigma • ZeroCash • Hawk	**Reading:** Enigma - Guy ZeroCash - Madars Elaine Shi's - Hawk **Discussion:** We want to do serious research on blockchain regarding issues like privacy, but much of this field is not yet formalized. What are the next steps we need to take as a community of researchers to mature the research done on digital currencies? **Homework:** Project work
Week 11	Class cancelled - Thanksgiving week	
Week 13	Using blockchain to store/find non-financial data, bridging the physical and digital world Off-chain storage	
Week 14	Final Presentations	