Course: Blockchain and Money MIT

Course Description

This course is for students wishing to explore blockchain technology's potential use—by entrepreneurs and incumbents—to change the world of money and finance. The course begins with a review of Bitcoin and an understanding of the commercial, technical, and public policy fundamentals of blockchain technology, distributed ledgers, and smart contracts. The class then continues on to current and potential blockchain applications in the financial sector.

Instructor(s) Prof. Gary Gensler

MIT Course Number 15.S12

As Taught In Fall 2018

Level Graduate

Here I will document my studies and reading about blockchain technology in this course. I will answer the study questions for each lecture in the table of contents below.

Table of Contents

- Secondary Markets and Crypto-Exchanges
- A New Approach to Crypto-Exchanges and Payments
- Primary Markets, ICOs, and Venture Capital, Part 1
- Primary Markets, ICOs, and Venture Capital, Part 2
- Post Trade Clearing, Settlement, and Processing
- Trade Finance and Supply Chain
- Digital ID
- Second business write-up due by this class
- Conclusion

Good resource: Binance Academy - Blockchain & Crypto

Reading

Study questions:

I will answer the questions based on the lectures of this course.

- Introduction:
    - How to move value peer-to-peer without any trusted central intermediary?
        - **Answer**: Bitcoin: A Peer-to-Peer Electronic cash System.
        - ```
          "I've been working on a new eletronic cash system that's fully peer-to-peer, with no trusted third party."
          Satoshi Nakamoto
          ```
    - 1 - What is blockchain technology and why might it be a catalyst for change for the financial sector?
        - **My answer:** The blockchain technology is a consensus protocol used to create an append-only log, being a transaction ledger that can them be used to form an auditable database:
            - Secured via cryptography:
                - hash functions for tamper resistance and integrity
                - Digital signatures for consent
                - Consensus for agreement
                - Addresses 'Cost of trust' (Byzantine Generals problem)
                    - permissioned
                    - permissionless (**BITCOIN AND ETHEREUM BLOCKCKAIN**)
                - Distributed Consensus
    - 2 - What do you as a student wish to learn from this course, 'Blockchain and Money'?
        - **My answer:** In this course I hope to learn blockchain technology and the money rules basics and how this will be inserted in the financial world to the future.
          ```

- **What is money?**

  Adam Smith defines money by the roles it plays in society, in particular, how well it serves as:

  - **A store of value** with which to transfer purchasing power from today to some future time;
  - **A medium of exchange** with which to make payments for goods and services; and
  - **A unit of account** with which to measure the value of a particular good, service, saving or loan.

- **Reading**: The Impact of Blockchain Technology on Finance: A Catalyst for Change

- Money, Ledgers & Bitcoin

  - 1 - What do the roles (medium of exchange, store of value, & unit of account) and characteristics (durable, portable, divisible, uniform, acceptable & stable) of money mean historically and in today's digital economy?

    - **My answer:**
      - The roles and characteristics of money are essencial to reach the 'sound money' whose intrinsic value is determined by the laws of the markets, the supply and demand laws. The sound money allow the individual freedom and prosperity to the society. Today the sound money in one global digital economy will change the way the society works, allowing more people to participate in the financial world, thanks to the technology capable to reproduce the roles and caracteristics of the physical money in a digital world.

  - 2 - What is fiat currency, what are its ledgers, and how does it fit within the history of money?

    - **My answer:**
      - *fiat currency* is a currency used by nacional economies, that is not backed by a physical commodity like gold. *Ledger* is a book or collection of accounts in which account transactions are recorded, or is basically a way to record economic activity, social relationship or financial relationship. *fit within the history of money*: fit currency is a nature consequence that was born in the social economy relationship in the society, where the money is a social construct or social consensus mechanism.

  - 3 - How does Bitcoin fit within the history of money, the emergence of the Internet and failed attempts of cryptographic payment systems?

    - **My answer:**
      - The Bitcoin is a digital money or a peer-to-peer electronic cash system, being the first time in history of money was reproduced in a digital world, solving the classical problem in computer science, the 'double spending', by using the internet protocols and the cryptographic hash functions. This is a basically a payment system that allow to the participate to make ecomonic transactions that are record in one ledger, the blockchain, where we have the privacy and liberty garanted by the cryptographic.

Good ledger:

- Immutable
- Consistency
- Timestamp
- Ownership
- Acurracy
- Description of the transaction
- Comprehensive

Fiat Currency

- Social & Economic consensus.
- Represented by central bank liabilities & commercial bank deposits.
- Relies upon system of ledgerss integrated into fractional banking system.
- Accepted for taxes.
- Notes & Coins are legal tender for all debts public & privace.

- **Reading**:

  - A Brief History of Money
  - A Brief History of Ledgers

Characteristics of Money

- Durable
- Portable
- Divisible
- Uniform/Fungible

- **Blockchain Basics & Cryptography**

  - Bitcoin - Technical Features
    - Cryptography & Timestamped logs
      - Cryptographic Hash Functions
      - Timestamped Append-only Logs(Blocks) (immutable digital ledger, distributed)
      - Block Headers & Merkle Trees
      - Asymmetric Cryptography & Digital signatures
      - Addresses
    - Decentralized Network Consensus
      - Consensus through Proof-of-Work (PoW)
      - Network of Nodes
      - Native Currency (**Technological design feature that is part of the economic incentive system**, Bitcoin mining)
    - Transactions Script & UTXO
      - Transaction Inputs & Outputs
      - Unspent Transaction Output(UTXO)
      - Scripting Language

- 1 - What are the design features — cryptography, append-only timestamped blocks, distributed consensus algorithms, and networking—of Bitcoin, the first use case for blockchain technology?
  - **My answer:**
    - *cryptography* is methods and techniques to provide secure and protect information, in *append-only timestamped blocks* is a chain of block of data that are store in immutable way in time, using the concept called *distributed consensus algorithms*, where we do not have a central authority in the *networking*, where nobody has a control, but all the participants follow the protocol, the Bitcoin is a the first time in history that the blockchain technology are used to make money programming.
- 2 - What are cryptographic hash functions, asymmetric cryptography and digital signatures? How are they utilized to help make blockchain technology verifiable and immutable?
  - **My answer:**
    - *cryptographic hash function* is an algorithm that makes an arbitrary amount of data input and produces a fixed-size output of enciphered text called a hash value, or just 'hash'. *asymmetric cryptography and digital signatures* is a way to encrypt a message to protect the information send through the internet, and only the people with the digital signatures can access the information encrypted. The blockchain technology is formated by the design features, where we have a ledger that record the economic transactions between the participants, and the data for each block of transactions are hashed with the timestamp and pratically infeasible to change (immutable), for one transaction we have the asymmetric cryptographic between parties, where one party use your digital signature to sign the transaction with your private key to another party (public key), and only this party with the private key link cryptographic to this public key will have access to the Bitcoin. This ledger (history of all transactions) is public and everyone can verify the authenticity of the transaction.
- 3 - What is the double-spending problem and how it is addressed by blockchain technology?
  - **My answer:** Double-spending is a problem that arise in the beginning of the creation of the digital money, because the digital token can be spent more than once. For the first time this problem was solved by Satoshi Nakamoto with the creation of the *Bitcoin* using the blockchain technology.

- **Blockchain Basics and Consensus**

```
Blockchain - Proof-of-Work (PoW)

Innovation -- Chained proof of Work for Distribuited Network Consensus
              & Timestamping

#####################################################################
Block:
  - Previous Hash
  - Nonce
  Database:
    -------------------------------
```

```
    - Transactions (Tx)
    - ...
    -------------------------------

    Hash Function:
                      Known                   Known           Known
Unknown
     SHA256( Hash of previous block + Transactions hash + Timestamp +
Nonce)

     Output:
     ---> 0000.................................
   'Difficulty (zeros in the beginning of the hash)'

   Pow Difficulty
   - Targets 10 minutes average block generation time
   - Defined by the hashtag of leading zeros hash output
     requires to solve PoW
   - Adjusts every 2016 blocks - about every two weeks


   Genesis Block:
   Hash
    The hash of the genesis block: 2021-01-03
    000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

    has two more leading hex zeroes than were required for an early
block.

    ##
https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934
ff763ae46a2a6c172b3f1b60a8ce26f


    Hash:
00000000000000000008ee81042efa8e314ab763e386d182b35e218d771d0260
    Confirmations: 1
    Timestamp: 2021-06-20 11:01
    Height: 688289
    Miner: ViaBTC
    Number of Transactions: 1,077
    Difficulty: 19,932,791,027,262.74
    Merkle root:
b4ba6ed057353bd444012b9262f1ccb39c782052e56a71c7677a2e905813eafc

##############################################################################
###
```

```
 'Blockchain - Consensus supports longest Chain'
```

Bitcoin Mining Evolution

```
- Central Processing Units (CPUs) 2009-2010 >>> 2 - 20 MH/s
- Graphics Processing Units (GPUs) 2010-2013 >>> 20-300 MH/s
- Application Specific Integrated Circuit (ASICs) >>> 2013-2018 4 - 16
TH/s
```

Proof-of-Stack - Consensus Mechanism

```
# Alternative Consensus Protocols
- Generally Randomized of Delegated Selection of Nodes to Validate
next Block
- May have added mechanism to confirm Block Validators Work
- Proof of Stake (PoS) - Stake in Native Currency
- Proof of Activity - Hydrid of PoW and PoS
- Proof of Burn - Validation comes with Burning of Coins
- Proof of Capacity (storage or Space) - Based upon Hardware Space

Delefated selection May be based upon tiered System of Nodes

Major Permissionless Blockchain Applications still use Proof-of-Work
```

Network

```
- 'Full Nodes' - Store full blockchain & able to validate all
transactions
- 'Pruning Nodes' - Prune transactions after validation and aging
- 'Lightweight Nodes' - Simplified Payment Verification (SPV) nodes -
Stores Blockchain Headers only
- 'Miners' - Performs Proof of Work & Create new Blocks - Do not need
to be a Full Node
- 'Mining Pool Operators'
- 'Wallets' - Store, View, Send and Receive Transactions & Create Key
Pairs.
- 'Mempool' - Store of unconfirmed (yet validated) Transactions
```

- 1 - What is the Byzantine Generals problem? How does proof-of-work and mining in Bitcoin address it? More generally by blockchain technology?
    - **My answer:** Byzantine Generals problem arise in a group of generals, in command of a division of the Bizantine army, where the generals must decide whether to attack the city or retreat. Some generals can act as traitors being in disagreement with the others generals that have the intention to attack together to avoid losses. The communication between the generals by messenger to reach agreement on a strategy, maybe the message can be delayed or disappear. This problem describes nicely the ***distribuited consensus problem***, the generals are the computers and the traitors are faulty

computers, the messengers are data being sent over an unrealiable network. In a blockchain network, this problem is solve by the consensus algorithm used to agree on the ledger in Satoshi's Bitcoin is based on participants competing to win rewards denominated in bitcoin. Its breakthrough feature is a `proof-of-work` function, which imposes computation costs on each participant in the competition. The participants who engage in this proces are called **miners**. In essence, each miner collects a set of outstanding transactions, referred to as a `block`, while simultaneoously competing to find a randomly chosen string of numbers and letters. Once a miner finds the required string, they broadcast it, along with block, to the rest of the network and claim their reward, comprising a combination of freshly issued bitcoins and any fees that users have attached to transactions in the block. The competition for the next block begins, building on the chain of blocks that have come before. This is why the transaction ledger is known as a **blockchain**. Another important feature is that the bitcoin protocol includes an algorithm that automatically adjusts the difficulty of completing the next block as the overall processing power of the computing network changes. As more miners join the network, the difficulty of the cryptographic challenge rises, and as miners leave it becomes easier to solve.

- 2 - What other consensus protocols are there? What are some of the tradeoffs of alternative consensus algorithms, proof-of-work, proof-of-stake, etc.?
  - **My answer:** Yes, there are others consensus protocols with different approaches, like `proof-of-stack, proof of activity, proof of burn and proof of capacity`. There are a big differences between proof-of-work (PoW) and proof-of stack (PoS), because the PoW is important to provide a cryptography security and privacy to participants in the blockchain, e.g. the Bitcoin, but for this consensus protocol is necessary to invest a lot of money in computing power and electricity to mining, the blocks, where for design we have in principle a decentralized network that is the core fundamental written by Satoshi Nakamoto in the whitepaper, and by the way, this fundamental does not change over the 10 years and this make the "true value" of the BTC, the underlying blockchain technology. In the other hand, the PoS, the approach is different, the tradeoff now is not necessary computing power and a high energy supply to the protocol, i.e., the participants stack your coins and get a reward proporcional to the quantity of coins locked in the protocol, in this network we have a more centralized environment, that is not good in provide a security and privacy, like the PoW, because now we have a point of failure.
- 3 - How does Bitcoin record transactions? What is unspent transaction output (UTXO)? What is script code embedded in each Bitcoin transaction and how flexible a programming language is it?
  - **My answer:**

- **Blockchain Basics and Transactions, UTXO, and Script Code**

```
Transaction Format
```

```
-------------------------------------------------------------|
|Input                            |  Output                  |
|                                 |                          |
|Previous transaction ID          |  Value                   |
|Index                            |  Public Key              |
|Signature                        |  (Bitcoin Address)       |
-------------------------------------------------------------
|                       lock_time                            |
-------------------------------------------------------------

Previous transaction ID, Index, Signature -- Uniquely identifies an output

One satoshi 10^8 = 1 Bitcoin (BTC)

Coinbase Transaction

Reward for solving Proof-of-Work
- Only Input is the coinbase block reward
- Reward halves(1/2s) every 210,000 blocks
    - Originally 50 Bitcoins per block
    - 1º Halving (28 November 2012): 25 Bitcoins (50 % Mined)
    - 2º Halving (9 July 2016): 12.5 Bitcoins (75 % Mined)
    - 3º Halving (11 May 2020): 6.25 Bitcoins (87.5 % Mined)
    - 4º Halving (Expected 2024): 3,125 Bitcoins (96.875 % Mined)
    - 5º Halving (Expected 2028): 1.5625 Bitcoins (98.4375 %)
    - 6º Halving (Expected 2032 ): 0.78125 Bitcoins (99.21875)
- Output may not be used as a transaction input until another 100 Blocks
- Recorded as First Transaction in Merkle Tree
- May Include 100 Bytes of arbitrary data
    - Used for additional Nonce
    - Genesis Block included Headline from Financial Times:
        - 'The Times 03/Jan/2009 Chancellor on brink of second bailout for
banks
```

Unspent Transaction Output (UTXO) Set

- Bitcoin transaction outputs that have not been spent at a given time
    - Contains All currently Unspent transaction Outputs
    - Speeds up Transactions validation Process
    - Stored using a LevelDB database in Bitcoin Core called ´chainstate´

```
Bitcoin Script
    - Programming Code used for Transactions
  - Stack-based codem, with no loops (turning-complete)
  - Provides a Flexible Set of Instructions for Transanctions validation
and Signature Authentication
```

- 1. As many design features—public key cryptography, hash functions, append-only timestamped logs, digital cash, and proof-of-work—pre-date Bitcoin, what was the novel innovation of

Santoshi Nakamoto?
    - **My answer:**
- 2. How do economic incentives work within blockchain technology to maintain decentralized ledgers and avoid double spending? What are the incentives of consensus protocols and mining?
    - **My answer:**
- 3. Who is Satoshi Nakamoto? (Only kidding a bit.)
    - **My answer:**