Bitcoin and the Blockchain
Proposed Course Outline 2016-17

Faculty	Prof. Jayanth Varma Wing 7, Ext: 4867 email: jrvarma@iima.ac.in
Academic Associate	

Course Objectives:

In 2008, the pseudonymous computer scientist Satoshi Nakamoto introduced a cryptographic currency called the Bitcoin based on a novel decentralized ledger called the blockchain. While Bitcoin as a currency has had its ups and downs, there is growing interest in the decentralized ledger (the blockchain). The blockchain has potential applications in many different areas of finance which have traditionally used a centralized ledger maintained by a trusted party.

Banks, exchanges, depositories, central banks and regulators are all exploring potential applications of the blockchain to reduce costs, increase robustness and shorten settlement delays. A number of startups have received funding to build some of these applications.

The course is intended to cover:

- The cryptographic foundations of the blockchain and related technologies
- The role of the ledger in payment systems, clearing and settlement systems, and the inefficiencies associated with the traditional centralized ledger
- The most important applications of the blockchain and the associated software solutions.

The course is oriented towards finance professionals who need to understand the strategic implications of the blockchain in their respective fields. While a high level understanding the cryptographic foundations is essential for this purpose, the course is not focused on the mathematical and technical aspects of the cryptography.

Though the course is more about the blockchain than on Bitcoin, it takes the view that a study of the former must begin with an understanding of the latter. Apart from being the first application of the blockchain, the Bitcoin even now remains its most important exemplar.

Pre-requisites

The course tries to be self contained, but it assumes reasonable knowledge of basic finance, elementary mathematics and essential computing covered in the compulsory courses.

Evaluation:

Class Participation	20%
Two Group Projects	40%
(Lab project and Business Project)	
End Term Exam	40%

Session Outline

1. **Introduction**

   Read: Kariappa Bheemaiah (2015), Why Business Schools need to teach about the Blockchain: An overview of Cryptocurrency and Blockchain technology based business initiatives and models. Electronic copy available at `http://ssrn.com/abstract=2596465`.

2. **Cryptographic primitives**

   Read: A. Menezes, P. van Oorschot, and S. Vanstone (1996) "Overview of Cryptography", Chapter 1 in *Handbook of Applied Cryptography*, CRC Press, 1996 Electronic copy available at `www.cacr.math.uwaterloo.ca/hac`

3. **Traditional central ledger: Payment Systems**

   Read: Andrew Dent and Will Dison (2012) "The Bank of England's Real-Time Gross Settlement infrastructure, Bank of England Quarterly Bulletin 2012 Q3, Electronic copy available at `http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/qb120304.pdf`

   Bank for International Settlements, Committee on Payments and Market Infrastructures (2015), "Correspondent banking - consultative report", Electronic copy available at `http://www.bis.org/cpmi/publ/d136.pdf`

4. **Traditional central ledger: Clearing and Settlement**

   Read: Robert R. Bliss and Robert S. Steigerwald (2006), "Derivatives clearing and settlement: A comparison of central counterparties and alternative structures", *Economic Perspectives*, Vol. 30, No. 4, Fourth Quarter 2006. Electronic copy available at `http://ssrn.com/abstract=948769`

   Bank for International Settlements, Committee on Payment and Settlement Systems (1995) Section 3, "Alternative channels for settling cross-border trades", page 11-17, in "Cross-Border Securities Settlements", Electronic copy available at `http://www.bis.org/cpmi/publ/d12.pdf`

5. **Bitcoin and the distributed ledger**

   Read: Satoshi Nakamoto (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System", Electronic copy available at `https://bitcoin.org/bitcoin.pdf`

   Bitcoin FAQ. Electronic copy available at `https://bitcoin.org/en/faq`

6. **Public, Private and Permissioned ledgers**

   Read: Tim Swanson (2015) "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems", Electronic copy available at `http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf`

7. **Distributed ledger and settlement systems**

   Read: Euroclear and Oliver Wyman (2016) "Blockchain in Capital Markets: The Prize and the Journey", electronic copy available at `https://www.euroclear.com/en/campaigns/blockchain-in-capital-markets.html`

   DTCC (2016) "Embracing Disruption Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape", electronic copy available at `http://www.dtcc.com/news/2016/january/25/blockchain`

8. **Smart contracts**

   Read: Nick Szabo (1997) "The Idea of Smart Contracts", Electronic copy available at `http://szabo.best.vwh.net/smart_contracts_idea.html`

9. **Blockchain Case Study: Ripple**

   Read: "The Ripple Protocol: A Deep Dive for Finance Professionals", Electronic copy available at `https://ripple.com/ripple-deep-dive/`

10.	**Blockchain Case Study: Etherium**	
	Read:	“Ethereum Frontier Guide”, especially Chapter Electronic copy available at `https://ethereum.gitbooks.io/frontier-guide/`. Especially section on “Contracts and Transactions” also available at `https://ethereum.gitbooks.io/frontier-guide/content/contracts_and_transactions_intro.html`

Group Projects

Lab Project

The Lab Project would require each group to create a private blockchain with only the group members as permitted users with different sets of members having different roles:

- Administrators
- Ordinary users.
- Malicious users trying to subvert the block chain

The group would execute a series of transaction on their private blockchain.

Business Project

The group would identify an application for the blockchain in some area in finance (not covered in the course) and develop a business case for it. The project would include a description and justification for the type of blockchain to be used.