

# Introduction to Bitcoin

## Course Schedule

November 25, 2017

**Venue:** Jalvihar Guest House Seminar Hall, IIT Bombay

Time	Topic
0900 – 0930	Registration
0930 – 1000	Tea and Networking
1000 – 1055	<ul style="list-style-type: none"><li>• Challenges in decentralized digital currencies</li><li>• The double spending problem</li><li>• Bitcoin's blockchain</li><li>• SHA-256 hash function</li><li>• Bitcoin mining</li><li>• Q&amp;A</li></ul>
1100 – 1155	<ul style="list-style-type: none"><li>• Mining difficulty adjustment</li><li>• Bitcoin supply regulation</li><li>• Tamper resistance of the blockchain</li><li>• Bitcoin transaction formats</li><li>• Bitcoin's scripting language</li><li>• Digital signatures for transaction integrity</li><li>• Q&amp;A</li></ul>
1200 – 1255	<ul style="list-style-type: none"><li>• Elliptic curves over real numbers</li><li>• Prime fields</li><li>• Elliptic curves over prime fields</li><li>• Bitcoin's elliptic curve</li><li>• Private and public keys in Bitcoin</li><li>• Key creation demo</li><li>• Q&amp;A</li></ul>
1300 – 1400	Lunch break
1400 – 1455	<ul style="list-style-type: none"><li>• Bitcoin addresses</li><li>• Base58 encoding</li><li>• Pay to Public Key Hash (P2PKH) Address</li><li>• P2PKH script execution</li><li>• Multisig script</li><li>• Pay to Script Hash (P2SH) Address</li><li>• P2SH Multisig script execution</li><li>• Q&amp;A</li></ul>
1500 – 1555	<ul style="list-style-type: none"><li>• Smart contracts</li><li>• Escrow contract</li><li>• Micropayments contract</li><li>• Q&amp;A</li></ul>
1600 – 1630	Tea/Coffee/Snacks and Networking