

Introduction to Bitcoin

Course Schedule

March 18, 2018

Venue: Jalvihar Guest House Seminar Hall, IIT Bombay

Time	Topic
0900 - 0930	Registration
0930 - 1000	Tea and Networking
1000 - 1125	<ul style="list-style-type: none">• Challenges in decentralized digital currencies• The double spending problem• Bitcoin's blockchain• SHA-256 hash function• Bitcoin mining
1125 - 1140	Tea break
1140 - 1300	<ul style="list-style-type: none">• Mining difficulty adjustment• Bitcoin supply regulation• Tamper resistance of the blockchain• Bitcoin transaction formats• Bitcoin's scripting language• Pay to Public Key Transaction
1300 - 1400	Lunch break
1400 - 1530	<ul style="list-style-type: none">• Elliptic curves over real numbers• Prime fields• Elliptic curves over prime fields• Bitcoin's elliptic curve• Private and public keys in Bitcoin• Key creation demo• Bitcoin addresses• Base58 encoding
1530 - 1535	Break
1535 - 1630	<ul style="list-style-type: none">• Pay to Public Key Hash (P2PKH) Address• P2PKH script execution• Multisig script• Pay to Script Hash (P2SH) Address• P2SH Multisig script execution• Smart contracts• Escrow contract• Micropayments contract
1630 - 1700	Tea/Snacks and Networking