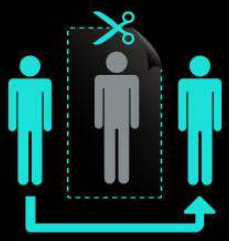
These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

General Studies
Bitcoins - Cryptocurrency

- Dr. Manishika Jain, NTSE Scholar, UGC NET JRF, CSIR NET JRF
Gold Medalist, Jawaharlal Nehru University, Delhi
Planner, City of Hillsboro, Oregon, USA



"If you can't explain it simply, you don't understand it well enough." - Albert Einstein

These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Why Use Bitcoin?

- Peer to peer
- Account cant be closed
- On digital wallet
- Simple as email
- Secured by Miners (rewarded for maintaining ledger)
- Changing finance
- Minimize transaction fee
- Cannot be frozen & blocked

Cryptocurrency - Anonymous

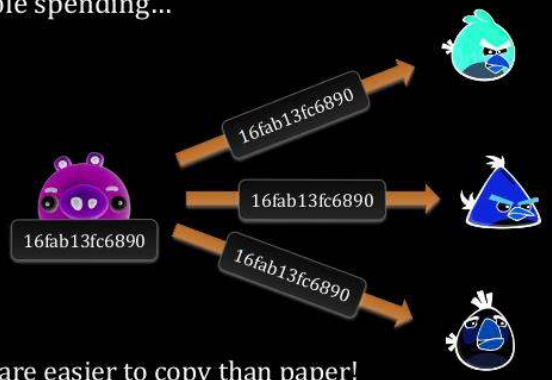
- Crypto = Hidden
- Key
- Signature
- Bitcoin/Altcoins – 1st decentralized cryptocurrency in 2009

These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Double Spending Problem

Main problem with the digital money

Double spending...



Bits are easier to copy than paper!

Open Ledger

- Chain of transactions
- Open & public
- Decide valid/not valid
- Centralized place
- Who is doing is private

These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Distributed Open Ledger

- Each can have copy of the ledger
- Many Copy – All synchronized (have same version)

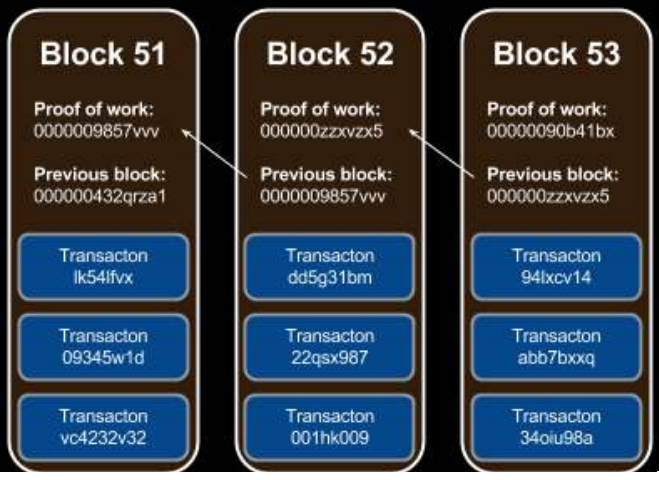
Miners

- Special nodes that can hold ledger
- Miners compete among themselves – to validate and add to ledger (check funds)
- Find key – take previous transaction & lock new transaction
- Invest computational power & time
- Gets financial reward (when solved)

These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Block Chain

- New group of accepted transactions
- 6 times every hour – blocks made
- Nonce: Arbitrary number may only be used once



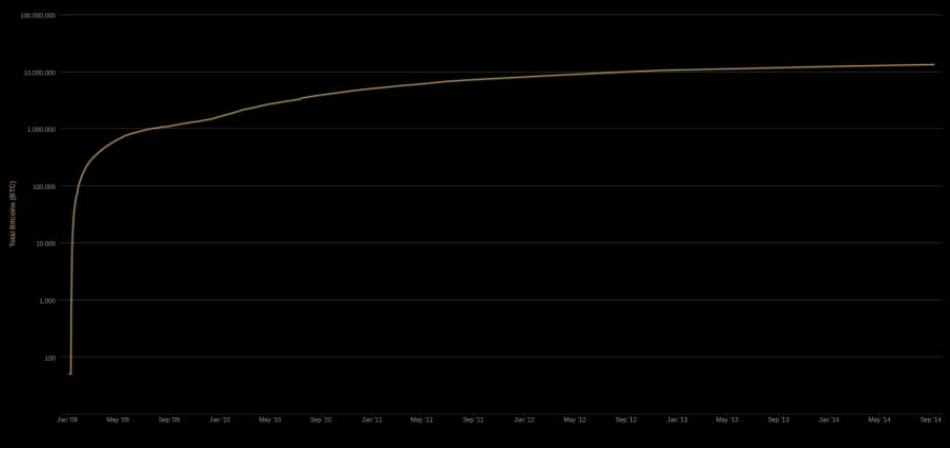
These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Block Chain – Public Distributed Ledger

- Its not bitcoin but backend of bitcoin
- Ledger is open and public
- Ledger exists in many nodes - decentralized
- Removes dependency on 3rd party
- No trusted entity
- Faster/Immediately
- Cheaper
- For new block – 12.5 BTC
- Every hour $12.5 \times 6 = 75$ BTC
- After 2.1 lakh block (4 years), amount of BTC is halved – ultimately zero BTC – only transaction fee

Bitcoin Circulation

- 21 million bitcoins in 100 years
- About over 13 million bitcoins in circulation by 2014
- 8 million bitcoins will be mined in next 95 years



These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

History of Cryptocurrency

- 1998: We-Dai – b-money – distributed electronic cash system
- BitGold by Nick Szabo
- 2009: Bitcoin - used SHA-256, a cryptographic hash function, as its proof-of-work scheme
- 2011: Namecoin
- 2011: Litecoin - used scrypt as its hash function
- Peercoin: proof-of-work/proof-of-stake hybrid
- 2014: Treasury

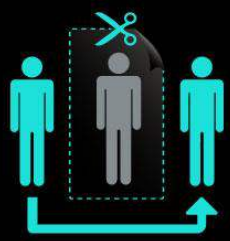
Algorithms

- SHA-2 (Secure Hash Algorithm 2) by NSA - cryptographic hash functions
- Scrypt: Password-based key derivation function – make it difficult to do hardware attacks

These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Bitcoin (BTC, XBT or ₿)

- Key and Signature
- Signatures are unique
- By Satoshi Nakamoto
- 31 May 2017: 1 bitcoin = $2257.96 or Rs. 143126.45
- Mathematically limited to 21 million bitcoins



Satoshi

- Satoshi / Austrian – one hundred million of BTC (smallest unit)
- Japanese character シ ("**shi**") - proposed
- Katakana symbol サ ("**sa**") - proposed
- Circled shi (㋿)
- Hiragana shi (し)

These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Why Bitcoin Fluctuates?

- Rate in 2010 ($0.08)
- USA (buy – uptick)
- Zambia (sell – downtick) 30 minutes later
- Decrease in Bitcoin rate by:
  - Merchants accepting Bitcoin
  - Miners "cashing out" to pay bills with fiat
  - Redemption of transmission bitcoin
  - Conversion of bitcoin salaries to fiat (increase in unused bitcoin)

Who Accepts?

- More than 1 lakh retailers
- Wallet applications
- Apple
- Dell
- Newegg
- e-Bay
- Dish Network

These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Global Scenario

- Japan – Bitcoin made legal (law passed)
- Australia – removed double tax on bitcoin users
- Bangladesh – Illegal – 12 years in jail
- Kyrgyzstan – Illegal (no prohibition from buying and selling)
- Ecuador – banned (creating its own virtual currency)
- Bolivia – Banned
- Vietnam – prohibits credit institutions from dealing in cryptocurrency

Bitcoin in India

- BTCXIndia: 1st bitcoin exchange in India with KYC and AML guidelines
- Unocoin
- Zebpay – 5 lakh app downloads & 2,500 users per day are added
- Fiat is needed to purchase Bitcoin to enter market in India – entry by donations, services or mining
- Still researching on bitcoin to make it legal
- Market acceptance, customer trust, investment security, money laundering, hawala

These Slides Accompany the YouTube Video Tutorial:
https://www.youtube.com/watch?v=lYW6Cw_VRHk

Bitcoin Thefts

- **Mt. Gox** –mtgox.com, short for "Magic: The Gathering Online eXchange' in 2006. World's leading bitcoin exchange in 2013-14 - 850,000 bitcoins were stolen which amounted to $450 million & finally bankruptcy declared
- **Bitfinex** - $72 million stolen in Hong Kong based exchange - customers would forfeit 36% of their holdings and be given "BFX tokens" instead that could be redeemed by the exchange or converted to shares in its parent company iFinex.