Bitcoins

Introduction to Bitcoins:

- virtual currency
- brought to life by:
  - internet
  - powerful computing resources
  - people willing for a new currency
- ease of use, can be used just like we send emails
- behind simplicity, lots of cryptography involved

- Similarity with traditional currencies
  - purchasing power
  - uses wallets for storage
  - getting widely accepted worldwide
  - inflation
  - theft of money happening
- Dissimilarities
  - not backed by any govt or financial agencies
  - govt cant keep a watch on its value or transactions
  - not physical, hence unlimited lifetime

Bitcoin exchange timeline:

- Oct 2009: 1309.03 BTC = $1
- July 2010: 12.5 BTC = $1
- Nov 2010: 2 BTC = $1
- Feb 2011: 1 BTC = $1
- June 2011: 1 BTC = $31.91
- April 2013: 1 BTC = $100
- Current exchange price:
  - 1 BTC = $ 121.6
  - 1 BTC = INR 7488

Cryptography

- uses ECDSA cryptography
- public and private keys of the owner associated with the coin
- hashcash function used for difficulty, and it uses the SHA-256 hashes

Addressing

- A bitcoin address contains 27-34 alphanumeric characters
- Can be generated by any user, any time
- Example- 31uEbMgunupShBVTewXjtqbBv5MndwfXhb
- uses base58 scheme
- like an email address
- are case sensitive and exact
- some characters are used for checksum to avoid typographical errors

Transaction

- Alice sending 1 Bitcoin to Bob
- Alice writes Bob's public key to the Bitcoin along with her own private key
- Bob gets the money through his private key
- The message is broadcast to whole network
- Users’ public-private keys will verify the transaction
- Whole transaction written to the Block-chain

Block Chain

- The transaction's broadcast message is appended to a chain, called block chain
- It is the transactional database shared by all nodes
- full copy of block chain contains every transaction ever executed on Bitcoins
- Each block contains the hash of previous block, and thus verifies the previous block
- Computationally impractical to create a fake transaction block, as it needs regenerating every block after it

Wallets

- Paper Wallets:
  - simple way to store bitcoins
  - installs a small app on pc or smart-phone
  - has multiple bitcoin addresses pairs
  - clean-boot computer and updated anti-virus/spyware for safety
- Hardware Wallets:
  - under construction
  - not yet operational, but are a major effort to provide enhanced security and usability

Securing the Wallets

- by default it uses AES-256-CBC to encrypt the private keys
- they are encrypted with an entirely random master key
- master key encrypted with AES-256-CBC with a key derived from passphrase using SHA512 and OpenSSL and random number of rounds
- when the wallet is locked, call for any kind of bitcoin modification will return an error
- To make the wallet secure against loss, we need:
  - to backup the data on secure online location or remote drive
  - archive it (with software like 7zip
  - encrypt it (with software like Truecrypt)
  - use shredding after usage

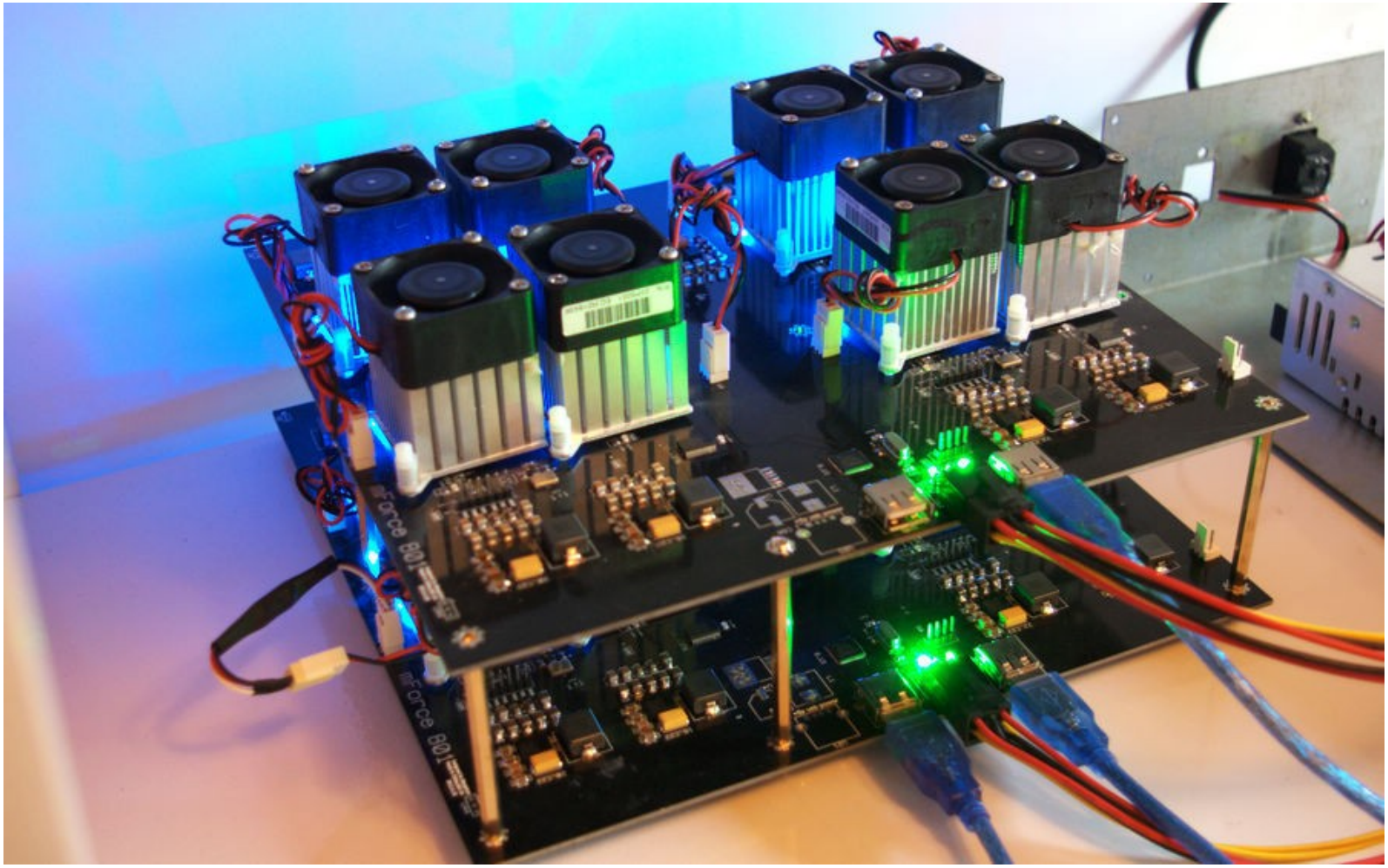
Mining

- is the process of adding transaction records to the block chain
- intentionally designed to be resource intensive and difficult so that the number of blocks found each day by miners remains steady
- why do people mine?
  - to earn bitcoins as reward
  - to get any transaction fee involved
- mining contracts for earning bitcoins
- so popular in west that data-centers are providing Mining-as-a-service (MaaS)

Hardware for Mining

- 1: CPU Mining
- 2: GPU Mining
- 3: FPGA Mining
- 4: ASIC Mining

FPGA Miner



Source: bitcointalk.org

ASIC Miner

Source: bitcoinmagazine.com

Strengths of Bitcoins

- easy to carry
- no taxes
- no third-party seizures
- no tracking
- no transaction costs
- much harder to steal

Weaknesses in Bitcoins

- vulnerable to Denial of Service
- time-jacking
- illegal content in block chain
- vulnerabilities and bugs
- easy packet sniffing
- energy consumption

References

- Bitcoin wiki – en.bitcoin.wiki
- S Nakamoto “Bitcoins – A peer to peer electronic cash system” www.bitcoin.org
- “The bitcoins arms race is on” spectrum.ieee.org
- R Grinberg “Bitcoin: An innovative alternative digital currency”
- S Barber, X Boyen, E Shi and E Uzun “Bitter to better – How to make bitcoin a better currency”