Blockchains

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-17/

Overview

1. Trend: Centralized to Decentralized
2. Importance of Blockchain
3. Technical Innovations of Bitcoin
4. Blockchain Applications

Wedding

Wedding

- ❑ **Centralized**
- ❑ **Decentralized**

- ❑ Centralized registry
- ❑ Single point of failure
- ❑ Easier to hacked

- ❑ Decentralized
- ❑ No single point of failure
- ❑ Very difficult to hack

Blockchains

- **What** it allows:
  - Two complete strangers can complete a transaction without a third party
  - 1st Generation: Transaction = Money transaction
  - 2nd Generation: Contracts, Agreements, Property, …
  - Revolutionizing and changing the way we do banking, manufacturing, education, computer networking, …
- **How** is it done?
  - A singly linked chain of blocks of verified signed transactions is replicated globally on millions of nodes
  - You will have to change millions of nodes to attack/change
- **Who** is interested in it: Banks, ISPs, Venture Capitalists, … ⇒ Researchers, students, …

Blockchain (Cont)

- Proven:
  - Cryptographically secure
  - Hacker proof
  - No single point of failure
  - Achieves **decentralized** "consensus"

Examples of Centralized Systems

- **Banks**: Allow money transfer between two accounts
- **Currency**: Printed and controlled by the government
- **Stocks**: Need brokers and clearing house (NY stock exchange, Bombay Stock Exchange, …)
- **Credit Card companies**
- In all cases:

1. There is a central third party to be trusted
2. Central party maintains a large database of information
   ⇒ Attracts Hackers
3. Central party may be hacked
   ⇒ affects millions
4. Central party is a single point of failure.
   Can malfunction or be bribed.

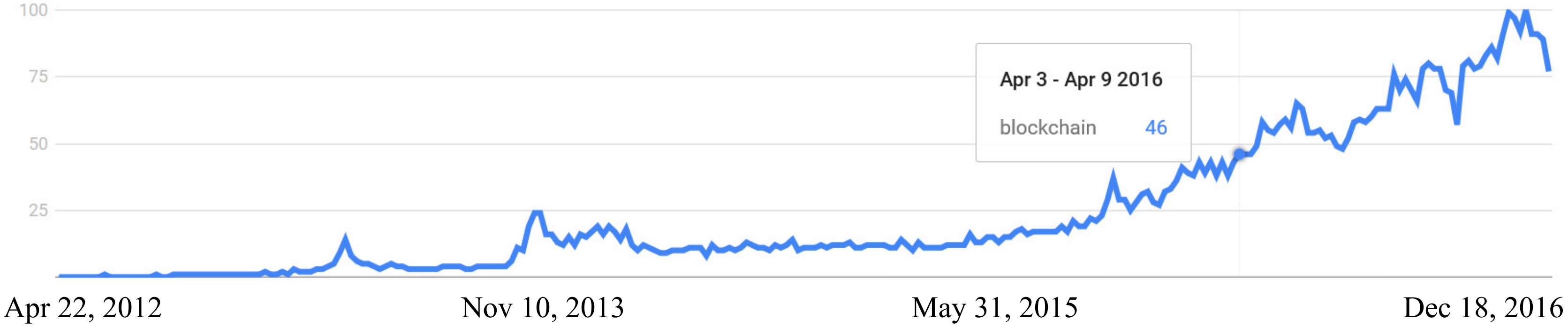
Trend: Centralized to Decentralized

- **Trend**: Make everything decentralized with no central point of control
- You can send money to your friends in Russia, China without their governments knowing it
- You can make a wedding contract, Property contract
- Decentralized systems are
  1. More reliable: Fault tolerant
  2. More secure: Attack tolerant
  3. No single bottleneck ⇒ Fast
  4. No single point of control ⇒ No monopoly ⇒ Cheaper
- Libertarians decided to build a totally decentralized system with no central authority. Blockchain is one way to do this.

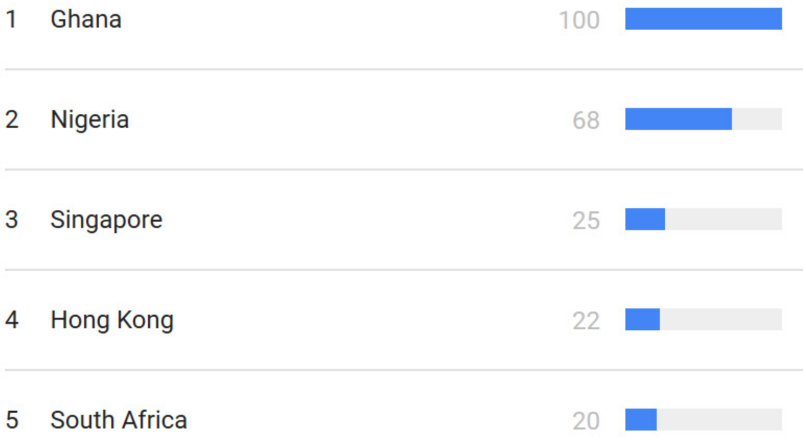
Fifth Disruptive Computing Paradigm

1. **Mainframes**: IBM
2. **Personal computers**: Microsoft
3. **Internet**: Netscape, …, Google
4. **Mobile and social networking**: Apple, Facebook
5. **Blockchains**: Decentralized money exchange, micro financing, contracts, machine economy (IoT payments)

Google Trend: Blockchains

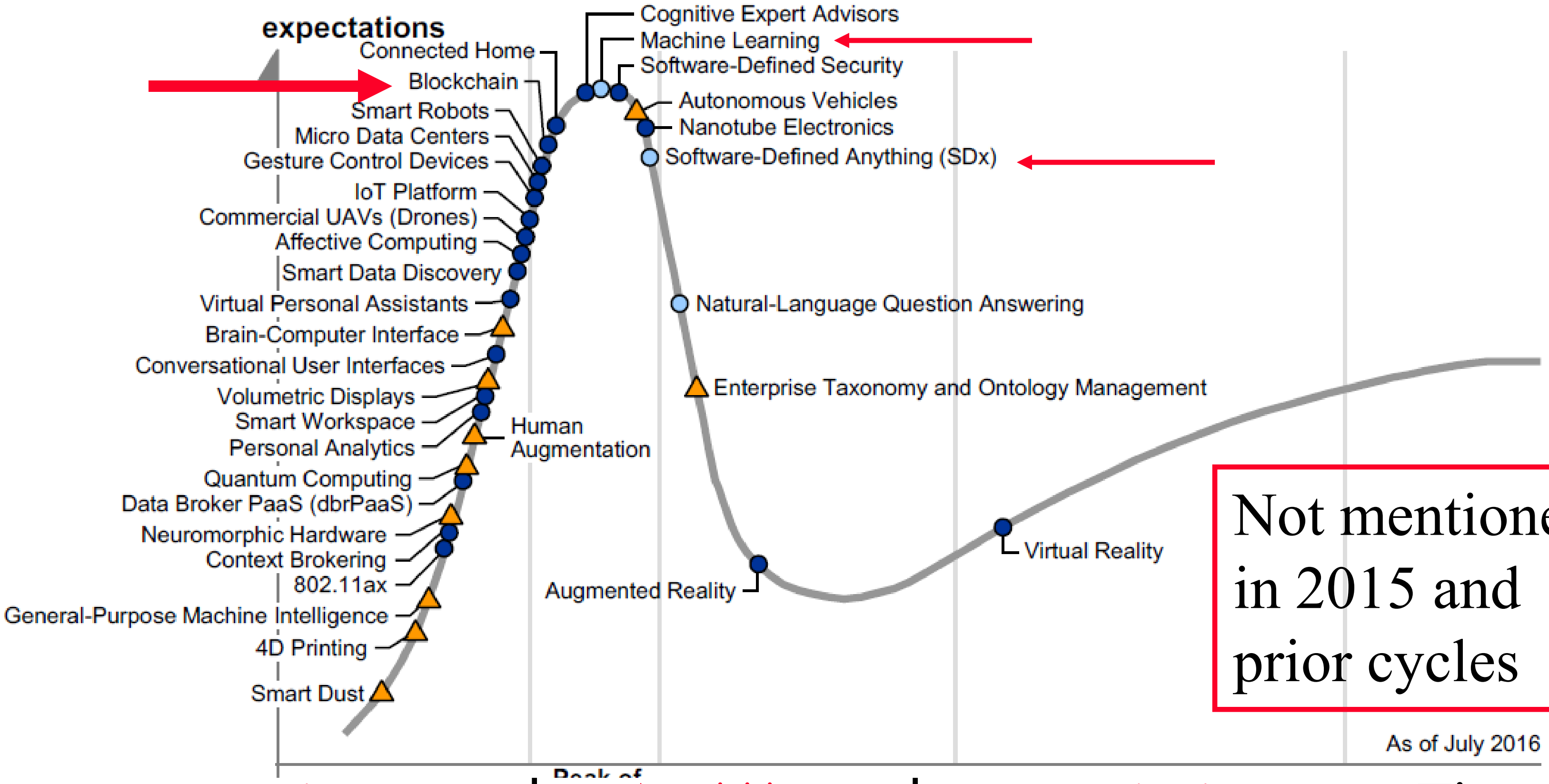


- Countries with most interest in Blockchains:



1	Ghana	100	🟦
2	Nigeria	68	🟦
3	Singapore	25	🟦
4	Hong Kong	22	🟦
5	South Africa	20	🟦

Gartner's Hype Cycle of Emerging Tech 2016



Not mentioned in 2015 and prior cycles

VC investment | Acquisitions By large corporations | Mass Production

Time

Ref: M.J. Walker, B. Burton, M. Cantars, "Hype Cycle for Emerging Technologies, 2016," Gartner Report, G00299893, July 2016

Blockchain Origin: Bitcoin

- Blockchain is the technology that made Bitcoin secure
- Blockchain was invented by the inventor of Bitcoin
- After Bitcoin became successful, people started looking into the technology behind Bitcoin and found:
  - Blockchain is the key for its success
  - Blockchains can be leveraged for other applications

Bitcoin

- First Successful Virtual Currency
- Has survived 6 years and has become legal in several jurisdiction
- Decentralized: No one company or government controls it
  - Decentralized Transaction Verification
  - Decentralized Ledger (accounting book)
  - Decentralized Mint to make new coins
  - Decentralized peer-to-peer network
- Has been designed to control over-minting, double-spending, counterfeiting
- 1 BTC = 1199.99 USD (April 17, 2017) was 620.04 USD (Sep 9, 2016)
- 10^{-8} BTC = 1 Satoshi = 0.0012 cents
- 16,279,313 BTC (April 16, 2017)
- Total 21 Million BTC will ever be generated.

Ref: https://coinmarketcap.com/

30,000+ Vendors Accept Bitcoins

- ❑ Dell
- ❑ Newegg.com
- ❑ TigerDirect
- ❑ Apple’s App Store
- ❑ Sears
- ❑ K-Mart
- ❑ Square
- ❑ Subway
- ❑ **Safer than using credit cards**

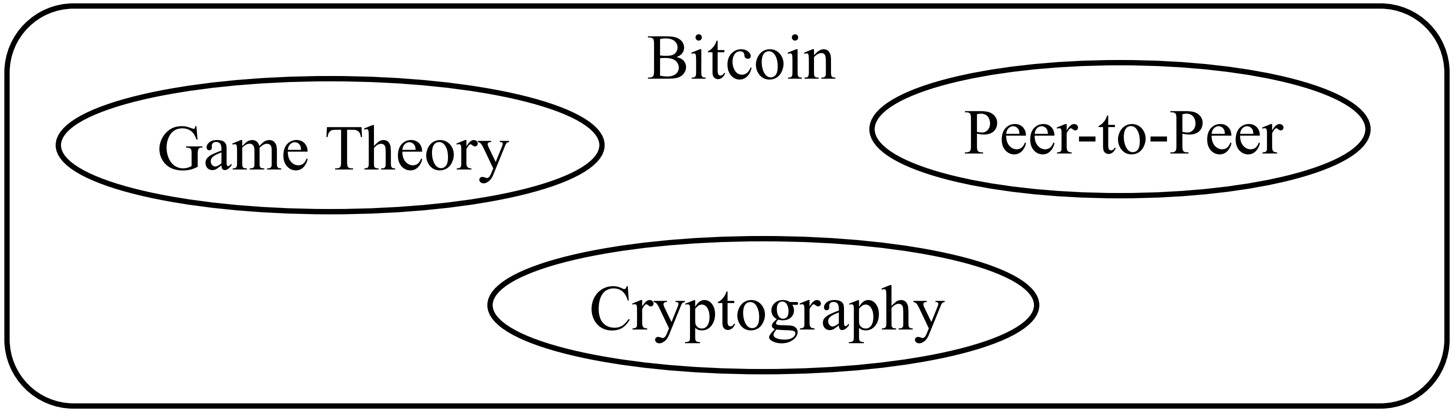
Ref: https://99Bitcoins.com/who-accepts-Bitcoins-payment-companies-stores-take-Bitcoins/

Bitcoin History

- Satoshi Nakamoto published a *whitepaper* in 2008. How to do direct transfer of money without involving a 3rd party.
- He also published complete reference code to transact, store, and mint Bitcoins. Made the software open source.
- He supported the software and answered all questions for 3 years and then disappeared
  (may be because he was rich or fearful)
- P2P Network:
  - Nodes come up and leave at random
  - Packets are delayed, lost, duplicated
  - Some nodes are malicious
- As long as a majority of CPU power is not with attackers, the system works ⇒ Proof of Work

Ref: Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://Bitcoin.org/Bitcoin.pdf

Bitcoin Technology



- Bitcoin = Game Theory + Cryptography + P2P
- P2P: Information is stored throughout the global Internet
- Cryptography: Digital Signature, Message Authentication, Asymmetric Public/Private Key encryption, Hashing
- Game Theory: All activities are Win-Win.
  ⇒ People who store the chain, who mint the coin, all get paid.

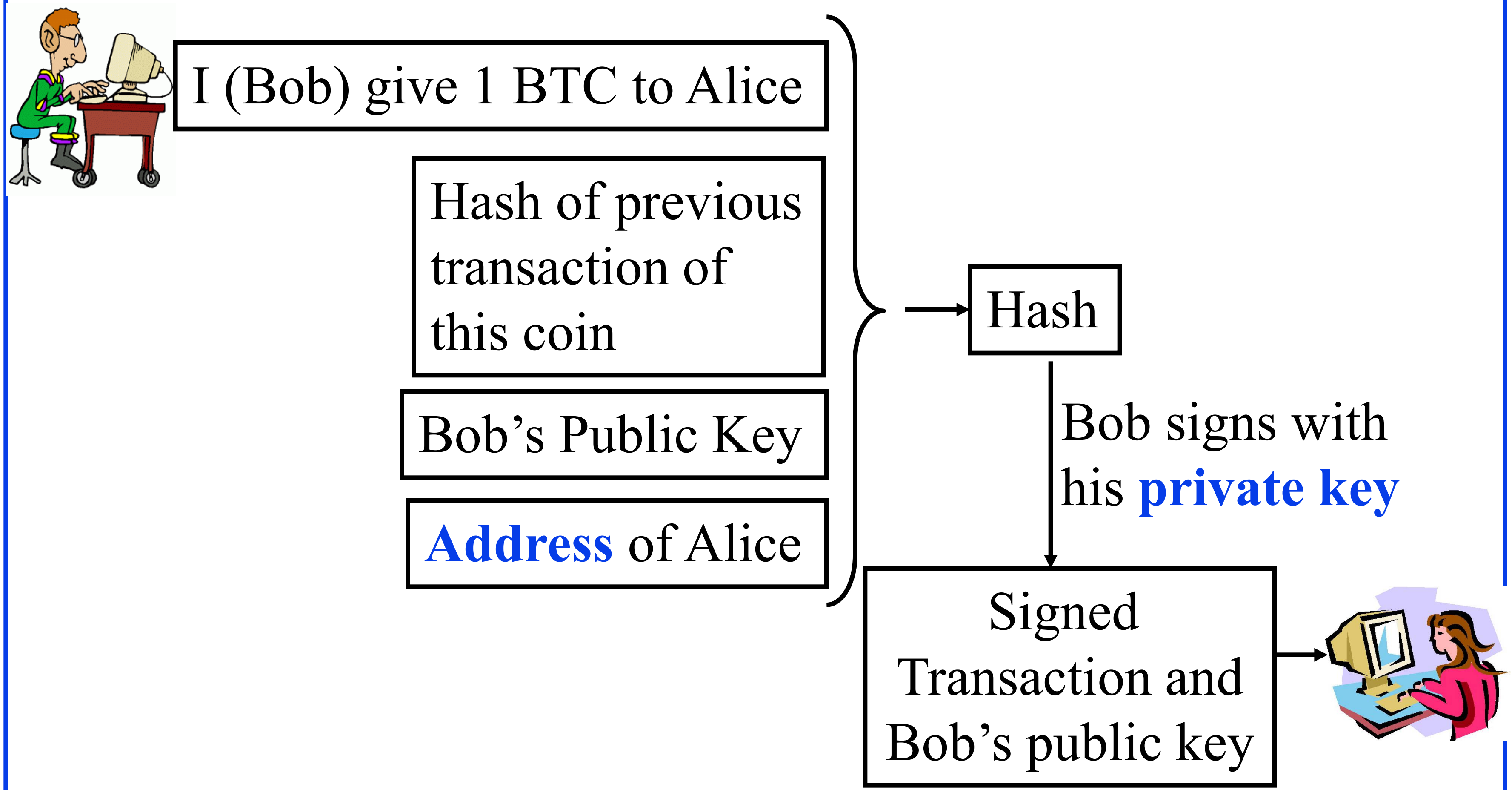
Bitcoin Wallet

- ❑ Program to manage your incoming/outgoing Bitcoins
- ❑ Allows generating new addresses and public/private key pairs
- ❑ Keep track of holdings of your different addresses
- ❑ Similar to Apple Wallet, Google Wallet, …
- ❑ Numerous apps on Apple's App store or Google Play Store

Coinbase Blockchain Bitcoin Free Bitcoin Billionare BitWallet Airbitz

Transaction

- Bob gives 1 BTC to Alice



I (Bob) give 1 BTC to Alice

Hash of previous transaction of this coin

Bob’s Public Key

Address of Alice

Hash

Bob signs with his **private key**

Signed Transaction and Bob’s public key

Ledger

- Solution to Double Spending

From	Amount	To
Bob	1 USD	Alice
Cash	2 USD	Grocery
Electronics	5 USD	Cash
…	…	…

Bob's Account
Balance=Balance-1

Alice's Account
Balance=Balance+1

- Maintained by a bank or in a personal computer
- Problem: It can be hacked.

Decentralized Ledger

- Copy 1

From	Amount	To
Bob	1 USD	Alice

- Copy 2

From	Amount	To
Bob	1 USD	Alice

…

- Copy *n*

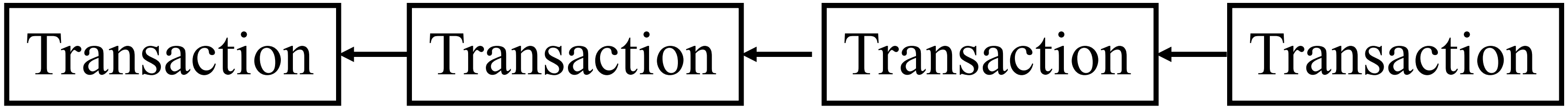
Bob's Account
Balance=Balance-1

Alice's Account
Balance=Balance+1

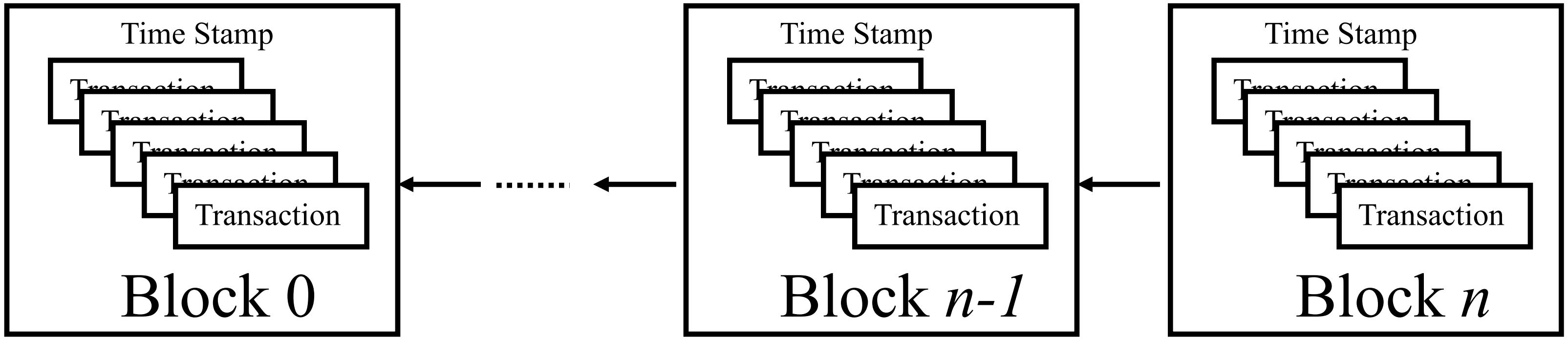
Cannot be hacked unless 51% copies are hacked.

Blocks

- Transaction Chain:


Transaction ← Transaction ← Transaction ← Transaction

- Problem:
  - Too many transactions ⇒ Chain too long
  - Takes too long to find and verify a transaction
- Solution: Combine several transactions into blocks of verified transactions


Time Stamp
Transaction
Transaction
Transaction
Transaction
Transaction
Block 0

....

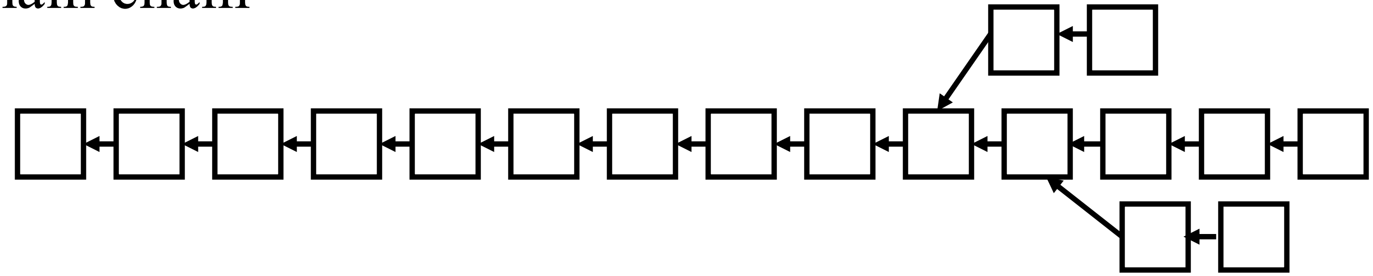
Time Stamp
Transaction
Transaction
Transaction
Transaction
Transaction
Block *n-1*

Time Stamp
Transaction
Transaction
Transaction
Transaction
Transaction
Block *n*

Blockchains

- ❑ Block maker (Miners) ensures that all transactions in the block are valid
- ❑ Miners have significant computing power
- ❑ Miner with the highest computer power wins. His/her block is added to the end of the chain

- ❑ Miner is rewarded. He/She is allowed to mint a few new coins and keep them
- ❑ Proof of computing power ⇒ **Proof of work** ⇒ Solve a puzzle
- ❑ Chain with the highest cumulative difficulty is selected as the main chain



Bitcoin Address

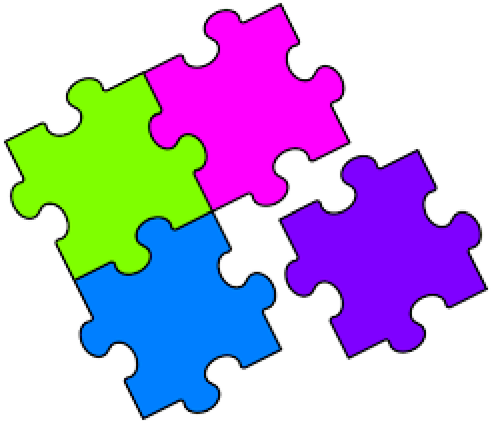
- Addresses=RIPMD160(SHA-256(Public Key))
- Addresses are encoded with Base-58 encoding
  (10 digits + 26 uppercase + 26 lower case – 4 (0, O, 1, I)
- Base58 Check Encoding: 4-byte checksum is appended.
  Checksum=First 4 bytes of SHA256(SHA256(Prefix+Data)
- Prefix is 0x00 = version
- After encoding a 1 is added to indicate that it is an address
- Always start with 1
- Generally presented as a QR Code

Pseudo-anonymous

- Using a nonce, you can generate a new public/private key pair
- SHA-256 hash of the public key is your address
- All transactions are between two addresses
- You can have as many addresses as you like
- You do not need to disclose your name, ID, or physical address ⇒ Pseudo anonymous
- If a transaction touches the physical world, your identity is disclosed, e.g., when buying your first Bitcoin with your credit card

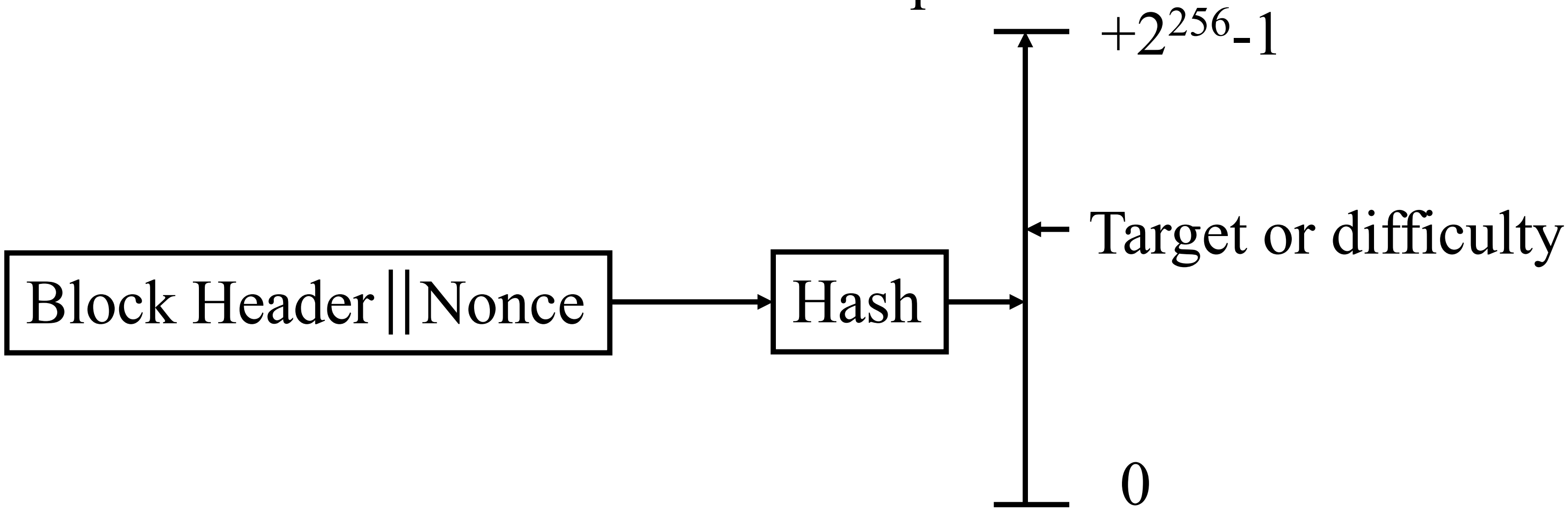
Proof-of-Work

- When someone requests a service, ask them to do something that is difficult for the requester but easy to verify for the server. Captcha is one example
- Bitcoin requires a proof that you can compute faster than others
- A puzzle is given and the node that solves it first wins
- Puzzle is such that it can be solved in ~ 10 minutes
  ⇒ Puzzles are being made harder as the computing power is increasing with Moore's Law



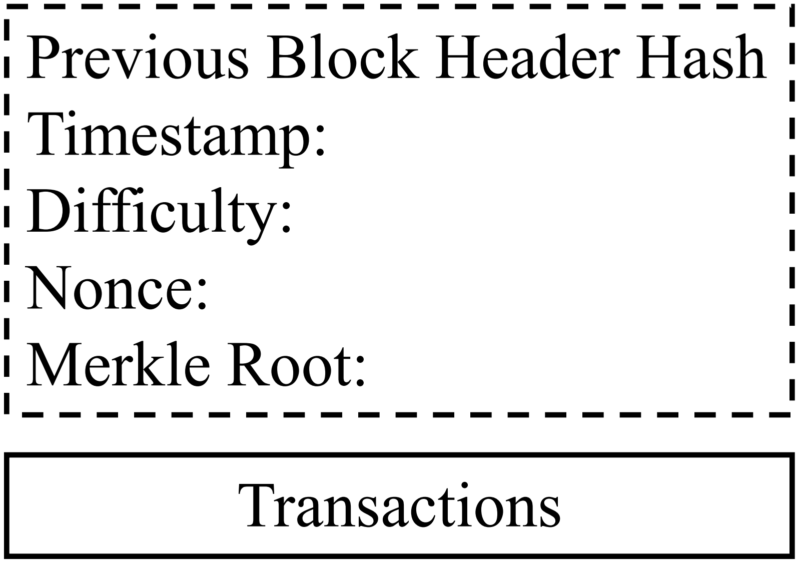
Puzzle

- Find a nonce that will make the hash of the block header less than a specified target
- Lower target ⇒ More difficult to find
- Puzzle can be made harder/easier by specifying a higher or lower target
- Target is adjusted by all miners every 2 weeks (2016 blocks) so that it takes 10 minutes to solve the puzzle.



Block Structure

- Block header contains a double-hash of the previous block header, a hash of the root of the Merkle tree of transactions in the block, a time stamp, Proof of work, nonce



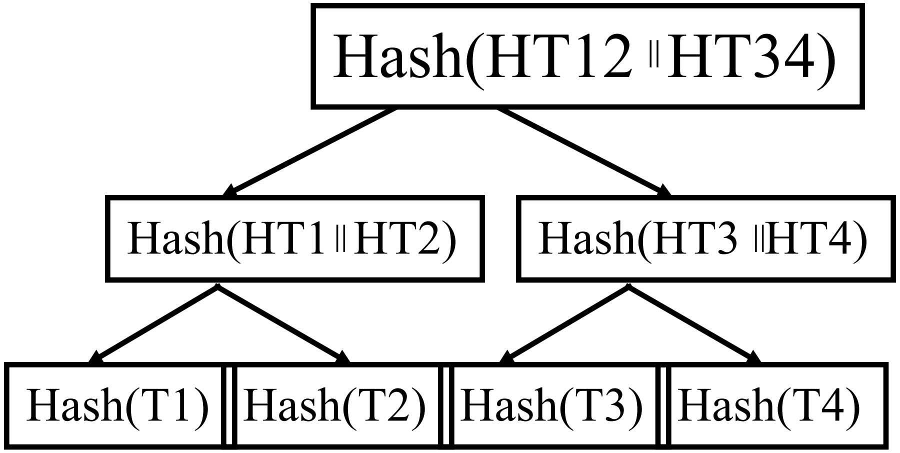
Previous Block Header Hash
Timestamp:
Difficulty:
Nonce:
Merkle Root:

Transactions

Ref: A. M. Antonopoulos, "Mastering Bitcoin," O'Reilly, 2015, 274 pp.

Merkle Tree

- A Binary hash tree to efficiently summarize and verify the integrity of large sets of data
- Hashes of the transactions are stored in the tree
- Parents contain hash of the concatenation of children
- Takes $\log_2(n)$ comparisons to find the transaction among n



Ref: A. M. Antonopoulos, "Mastering Bitcoin," O'Reilly, 2015, 274 pp.

Smart Property

- Bob: I give $100 to Alice if IBM stock goes below $5
  - Locking script: if IBM stock < $5 Return True
  - Unlocking script: IBM stock price is $4
- Property exchange happens if certain conditions are satisfied. Conditions can be checked automatically
  ⇒ Allows trustless exchanges
- **Smart Contracts**: Not just buy/Sell. Any agreement.

Potential Blockchain Applications

- **Financial**: Currency, Private equities, Public equities, Bonds, Derivatives, Commodities, Mortgage records, Crowd-funding, Micro-finance, Micro-charity
- **Public Records**: Land titles, Vehicle registries, Business license, Criminal records, Passports, Birth certificates, Death certificates, Building permits, Gun permits
- **Private Records**: Contracts, Signatures, Wills, Trusts, Escrows
- **Other Semi-Public Records**: Degree, Certifications, Grades, HR records, Medical records, Accounting records
- **Physical Asset Keys**: Apartment keys, Vacation home keys, Hotel room keys, Car keys, Rental car keys, Locker keys
- **Intangibles**: Patents, Copyrights, Trademarks

Ref: http://ledracapital.com/blog/2014/3/11/Bitcoin-series-24-the-mega-master-blockchain-list

Networking Applications

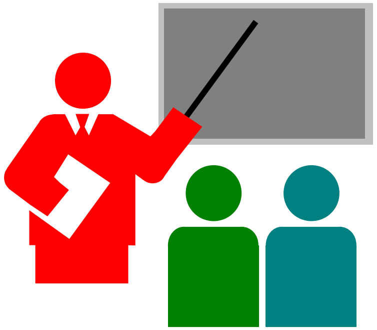
- **NameCoin**: A decentralized key-value registration and transfer platform using blockchains.
  - A decentralized **Domain Names Registry**
  - To eventually replace *Internet Corporation for Assigned Names and Numbers* (*ICANN*)
  - .bit domain names
  - Includes its own currency to pay for registration
- DARPA issued a RFP for Secure Decentralized Messaging using Blockchains
- **InterPlanetary File System** (IPFS): Decentralized secure file serving
- **Storj**: Decentralized secure cloud storage using blockchains
- **OneName**: Digital identity. Authenticatio using Wallet

ISP Opportunities

- Mobile Money
- Billing
- Digital Asset transactions
- Roaming
- Connectivity provisioning
- M2M, IoT, Smart Cities
- Identity Management

Ref: http://www.analysysmason.com/Research/Content/Comments/nine-blockchain-opportunities-Jun2016-RDMY0/

Summary



1. Current trend is to make everything decentralized
2. Bitcoin is a decentralized currency.
3. Blockchain 1.0 is used to global consensus on Bitcoin transactions.
4. Blockchain 2.0 allow sophisticated contracts making it useful for many applications
5. Opportunity for startups, venture capitalists, and researchers

Lab 26: Blockchains

- You will need to use python to do this lab
- Make sure that you have python installed
  - MacOS or Linux: brew install python3 (http://python-guide-pt-br.readthedocs.io/en/latest/starting/install3/osx/)
  - Windows: https://www.python.org/downloads/windows/
- Install blockchain API from https://github.com/blockchain/api-v1-client-python
- Read the blockexplorer and statistics documentations. This lab is all around those two documentations.
  - blockexplorer: https://github.com/blockchain/api-v1-client-python/blob/master/docs/blockexplorer.md

Statistics about Bitcoin

- statistics: https://github.com/blockchain/api-v1-client-python/blob/master/docs/statistics.md

Statistics about BitCoin

- Start python. Write commands for each of the following:
- Import statistics from blockchain
- Get the latest network statistics
- Get the following information (with command used)
  - How many bitcoins have been mined
  - Minutes between blocks
  - Difficulty
  - Number of mined blocks
  - Block size
  - Total blocks numbers

Blocks Structure

- Import blockexplorer from blockchain
- Get the block with id
  “000000000000000016f9a2c3e0f4c1245ff24856a79c34806969f5084f410680”
- Answer the following questions about the above block (with command used)
  - What is the hash
  - What is the nonce
  - What is the Merkle root
  - Transactions in the block
  - What is the size
  - What is the index (height)
  - What is the received time of the block?

Transaction Structure

- Import blockexplorer from blockchain
- Get a transaction with id "d4af240386cdacab4ca666d178afc88280b620ae308ae8d2585e9ab8fc664a94"
- Answer the following questions about the above block (with command used)
    - What is the time?
    - What is the hash?
    - What is the block index (height)?
    - What is the size?
    - What is the address of the first input?
    - What is the address of the second output?

Further Reading

- A. M. Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," Oreilly, 2015, 272 pp.
- A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, "Bitcoin and Cryptocurrency Technology: A Comprehensive Introduction," Princeton University Press, 2016, 304 pp.
- M. Swan, "Blockchain: Blueprint for a new economy," Oreilly, 2016, 130 pp.
- S. Raval, "Decentralized Applications," Oreilly, 2016, 104 pp.
- D. Tapscott and A. Tapscott, "Blockchain Revolution," Portfolio Penguin, 2016, 348 pp.
- C. Skinner, "Value WEB: How FinTech firms are using Mobile and Blockchain Technologies to Create the Internet of Value," Marshall Cavendish Business, 2016, 424 pp.

Online Resources

- CoinDesk: Bitcoin News, Prices, Charts, Guides & Analysis, http://www.coindesk.com/
- Bitcoin magazine, https://bitcoinmagazine.com/
- CCN: Bitcoin, Blockchain, FinTech, & Cryptocurrency News, https://www.cryptocoinsnews.com/
- CoinTelegraph, https://cointelegraph.com/
- Bitcoin Stack Exchange, http://bitcoin.stackexchange.com/
- Let's talk Bitcoin, https://letstalkbitcoin.com/
- Epicenter - Weekly Podcast on Blockchain, Ethereum, Bitcoin and ..., https://epicenter.tv/
- Epicenter Bitcoin, https://epicenter.tv/
- Ethercasts, https://www.youtube.com/user/EtherCasts

Acronyms

API	Application Programming Interface
BTC	Bitcoin
CCN	Crypto Coin News
DARPA	Defense Advanced Research Project Agency
HR	Human Resources
ICANN	Internet Committee for Assigned Names and Numbers
ID	Identifier
IoT	Internet of Things
IPFS	Internet Protocol File System
ISP	Internet Service Provider
QR	Quick Response Code
RFP	Request for Proposal
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
SHA	Secure Hash Algorithm
USD	United States Dollar
VC	Venture Captial

Scan This to Download These Slides

Raj Jain

http://rajjain.com

Related Modules

CSE571S: Network Security (Spring 2017),
http://www.cse.wustl.edu/~jain/cse571-17/index.html

CSE473S: Introduction to Computer Networks (Fall 2016),
http://www.cse.wustl.edu/~jain/cse473-16/index.html

Wireless and Mobile Networking (Spring 2016),
http://www.cse.wustl.edu/~jain/cse574-16/index.html

CSE571S: Network Security (Fall 2014),
http://www.cse.wustl.edu/~jain/cse571-14/index.html

Audio/Video Recordings and Podcasts of Professor Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw