Blockchains: The Revolutionary Trust Protocol

RAJ JAIN

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

BEL Keynote at 22nd Annual International Conference on Advance Computing and Communications (ADCOM 2016), Bangalore, India, Sep 10, 2016

These slides and video recording of this talk are available at http://www.cse.wustl.edu/~jain/talks/bc_ad16.htm

Overview

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

Marriage

Marriage

- 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.

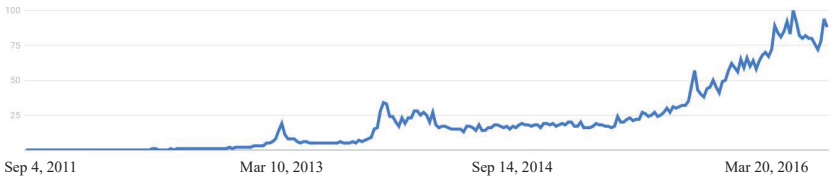
Trend: Centralized to Decentralized

- **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)

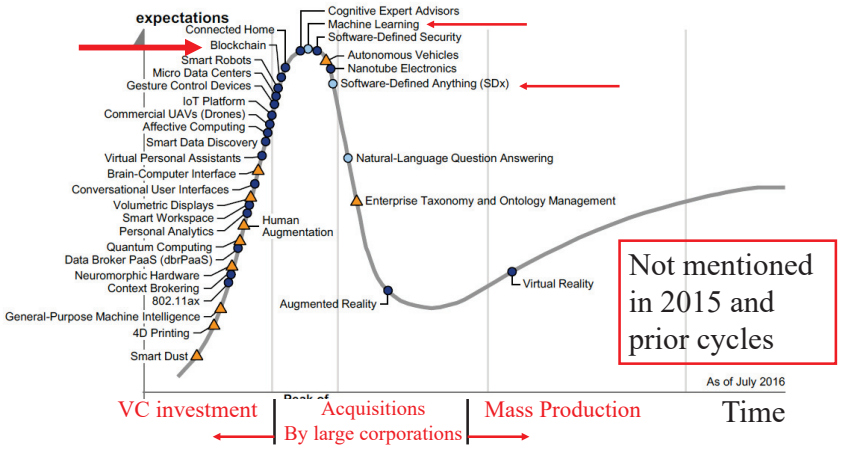
Google Trend: Blockchains



- Countries with most interest in Blockchains:

1	Ghana	100
2	South Africa	21
3	Singapore	20
4	Hong Kong	19
5	Switzerland	14

Gartner's Hype Cycle of Emerging Tech 2016



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

Venture Investments on Blockchains

- 2016 Q1: $160.70 M ⇒ $1B this year
- 2015: $488.08 M
- 2014: $362.53 M
- 2013: $95.05 M
- 2012: $2.13 M
- Sample Startups:
  - Bitt: Send and receive money
  - Elliptic.co: monitor illicit activities on blockchains
  - SurBTC: Chile's largest Bitcoin exchange
  - Simplex: Fraud prevention in Bitcoin exchanges and wallet applications

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 5 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 = 620.04 USD (Sep 9, 2016)
- 10^{-8} BTC = 1 Satoshi = 0.0006 cents
- 15,87664 BTC (Sep 9, 2016) = $10B

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**

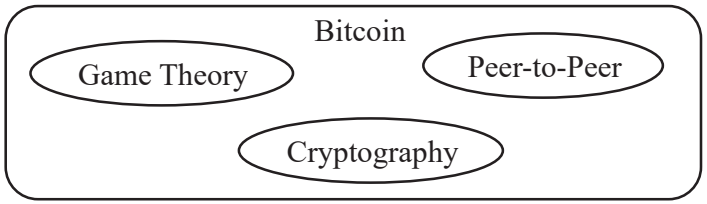
Ref: https://99Bitcoins.com/who-accepts-Bitcoins-payment-companies-stores-take-Bitcoins/

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

Bob's Account
Balance=Balance-1

Alice's Account
Balance=Balance+1

- Copy 2

From	Amount	To
Bob	1 USD	Alice

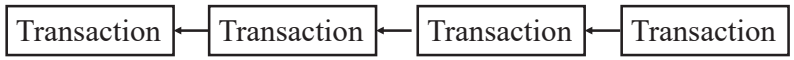
…

- Copy *n*

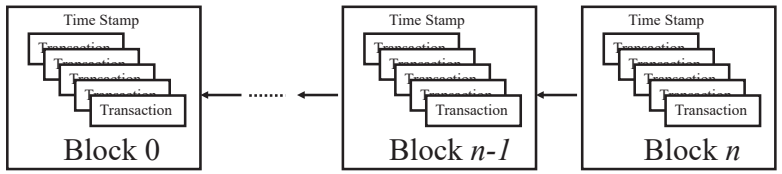
Cannot be hacked unless 51% copies are hacked.

Blocks

- Transaction Chain:



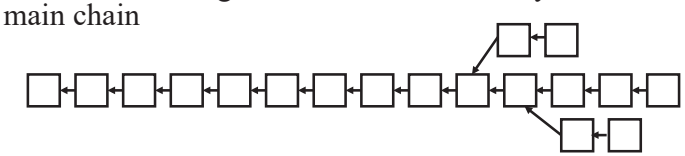
- Problem:
  - Too many transactions ⇒ Chain too long
  - Takes too long to find and verify a transaction
- Solution: Combine several transactions into blocks of verified transactions



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



Transaction Output

- Sender specifies a locking script that is executed when the specified money is spent by the recipient.
- Recipient supply a unlocking script that is executed after the locking script. If the result is TRUE, the transaction is valid.
- Most often the locking script is simply, "Pay-to-Public-Address-Hash". The unlocking script is generally a signature proving ownership of the Bitcoin address
- But more complicated locking and unlocking scripts can be written

Examples of Locking Scripts

- **Multi-Signature**: Two partners must sign to spend this money.
- A Forth like scripting language can be used to specify locking and unlocking scripts.
- **Pay-to-script-Hash**: Only the hash of locking script is specified. The recipient then supplies both locking script and unlocking script when spending the money
- No jumps in Bitcoin scripts ⇒ Avoid infinite loops
  - Not **Turing Complete =** Turing's tape machine.
- A new platform **Ethereum** allows Turing complete programs

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/

ISP Activities

- Verizon ventures invested in Filament – industrial assets communicate acting as autonomous agents using blockchains (August 2015)
- Orange Digital Ventures invested in Chain – blockchain solutions for financial services (September 2015)
- Du pilot program for secure transmission of electronic health records using blockchains (May 2016)

Summary

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

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

Scan This to Download These Slides

Raj Jain

http://bit.ly/blc_ad16