Blockchains: Networking Applications

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

Invited talk at the 38th IEEE Sarnoff Symposium
Newark, NJ
September 18, 2017

Audio/Video recordings of this talk are available at:

http://www.cse.wustl.edu/~jain/talks/blc_srnf.htm

Overview

1. Trend: Centralized to Decentralized
2. Importance of Blockchain
3. Blockchain Applications to Networking

Example of a Contract: Wedding

Wedding (Cont)

- Centralized

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

- Decentralized

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

©2017 Raj Jain

Blockchains

- **What** it allows:
  - Two complete strangers can complete a transaction without a third party
  - 1st Generation: Transaction = Money transaction
  - 2nd Generation: Transaction = Shares of
  - 3rd Generation: Smart 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: Banks, Hospitals, Venture Capitalists, …
  ⇒ Researchers, students, …

Blockchain Properties

- Achieves **decentralized** "consensus"
- No single trusted party required
- No single point of failure
- Cryptographically secure
- Hacker proof

©2017 Raj Jain

Blockchains: Centralized to Decentralized

- **Trend**: Make everything decentralized with no central point of control
- Two perfect strangers can exchange money, make a contract without a trusted third party
- 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
- Blockchain is one way to do this among **untrusted multi-domain** systems.

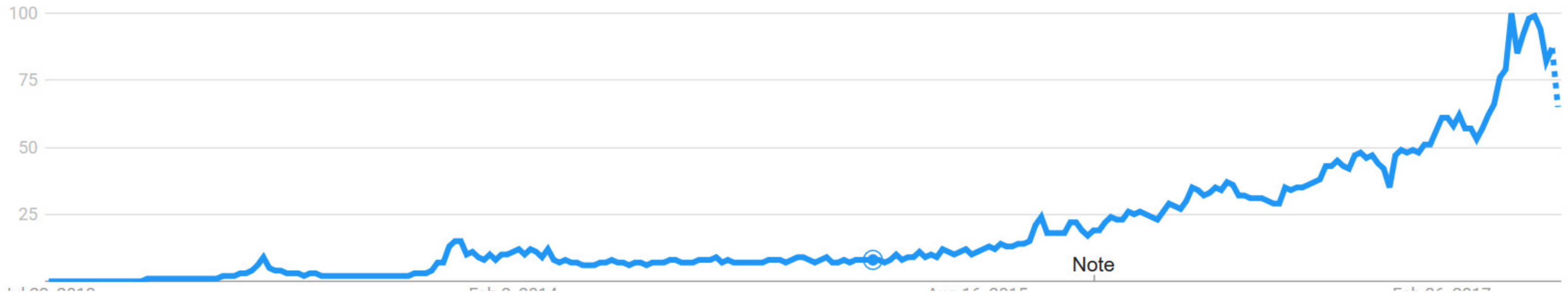
Time is a cycle: Distributed vs. Centralized debate

Examples of Centralized Systems

- **Banks**: Allow money transfer between two accounts
- **Currency**: Printed and controlled by the government
- **Stock Exchanges**: Needed to buy and sell stocks
- **Networks:** Certificate Authorities, DNS
- 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.

Ref: A. Narayanan, et al, “Bitcoin and Cryptocurrency Technologies,” Princeton University Press, 2016, 304 pp.

Google Trend: Blockchains

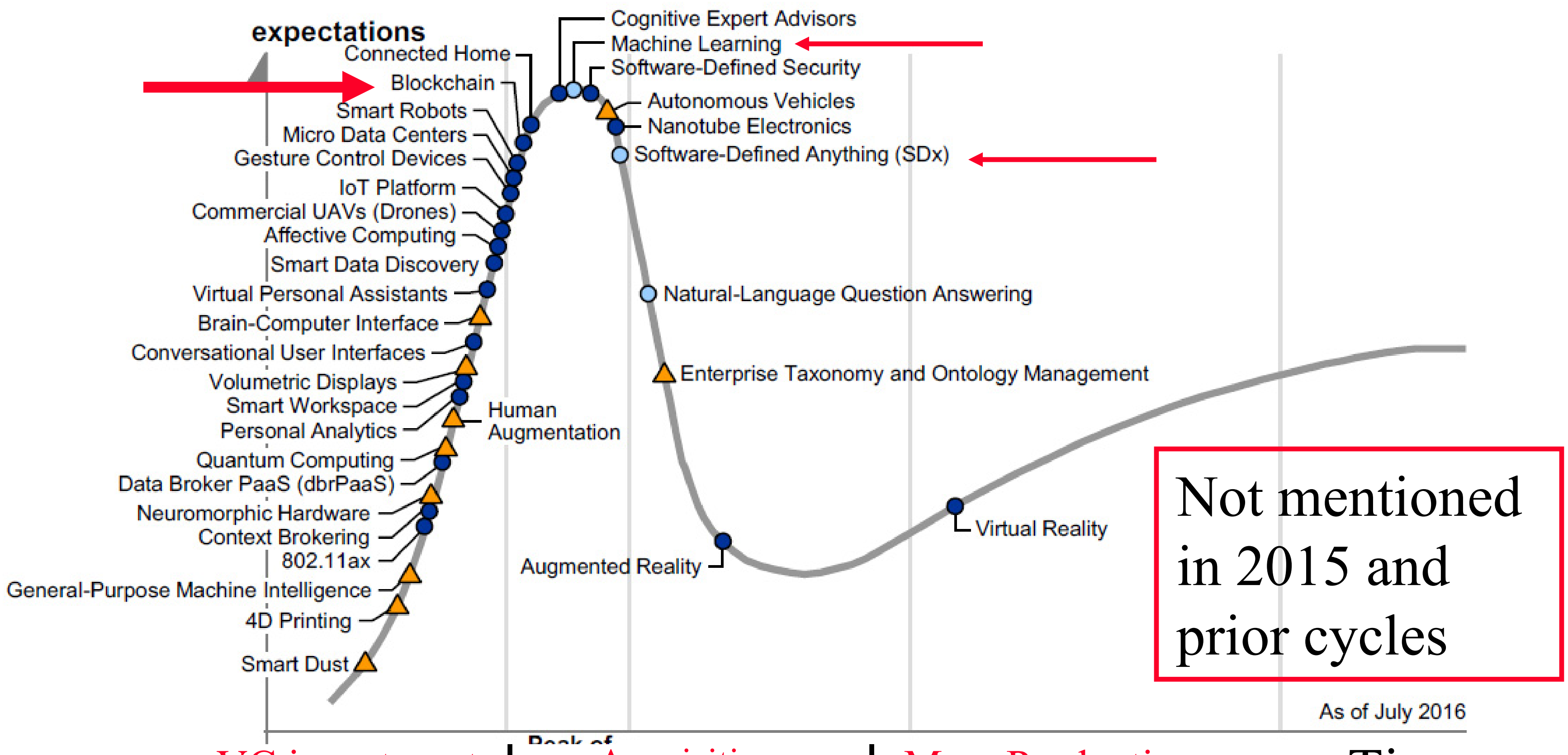


Jul 2012 Feb 2014 Aug 2015 Mar 2017

- ❑ 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

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 of Blockchains

- ❑ Multi-Domain Systems:
  - ➢ Multiple Cloud Service Providers
  - ➢ Multiple cellular providers
  - ➢ Multi-Interface devices: WiFi, Cell, Bluetooth, …
  - ➢ BGP: BGP Authentication
- ❑ Globally Centralized Systems:
  - ➢ DNS
  - ➢ Certificate Authorities

Explore blockchains for multi-domain/centralized systems

©2017 Raj Jain

Networking Applications (Cont)

- Public Key Infrastructure
  - Certificate Authorities issue certificates
  - Single Point of Failure
  - Diginotar – Dutch certificate authority was compromised in 2011)
- **NameCoin**: A decentralized key-value registration and transfer platform using blockchains.
  - A decentralized **Domain Names Registry**
  - .bit domain names
- DARPA issued a RFP for Secure Decentralized Messaging using Blockchains

Blockchains for Multi-Domain Large Scale Systems

Public Key Infrastructure

- Certificate Authorities issue certificates
  - Single Point of Failure
  - CA Keys are often compromised
    (Diginotar – Dutch certificate authority was compromised in 2011)
- Web of Trust: Anyone can issue a certificate
- Blockchain solution: Store user ID and public key
  - Blockstack
  - Certcoin

Data Provenance

- Keeping track of origin and history of movement of data among the databases or documents
- Traditional solution: Logging and auditing
- In a distributed cloud environment, centralized logging is required and is difficult
- Blockchains can be used to log the changes Miners verify the changes
  - ProvChain
  - SMARTDATA
- Also used in supply chains

Data Privacy

- Facebook and Google have massive amounts of personal information
- Who can access this information?
- Can someone do statistics on the database without having rights to personal information of all?
- Can the user hide its identity?
- Traditional Method: Access Control Lists (ACL) managed centrally (by Facebook and Google)
- Blockchains can be used to keep ACL and data stored in a distributed manner with no central control

Data Integrity

- Data has not been corrupted
- Traditional techniques: Digital Signatures and PKI, Replication
- In blockchains, data can not be tempered once committed to a block.
- Ericson provides a blockchain based integrity assurance service

Blockchain Challenges

- **Selfish mining**: Some one creating a large number of bad blocks keeping the miners busy with discards
- **Sybil Attacks**: Some one creating a large number of transactions denying service to legitimate users
- **51% Attack**: One entity owns the majority of miners
- Communication overhead
- Solving the puzzles for “Proof of Work” wastes computing resources

Alternatives to "Proof of Work"

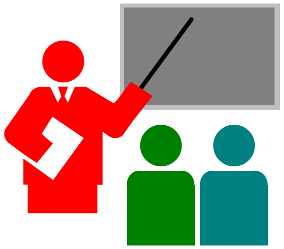
- **Proof of Space**: Computation is replaced by storage
- **Measure of Trust**: Most trustworthy miner wins
- **Minimum Block Hash** (rather than fastest) miner wins ⇒ More random
- **Proof of Importance**
- **Proof of Stake**

Blockchain Implementations

- **Open Source Implementations**:
  - Bitcoin
  - Etherum
  - Hyper Ledger
- **Commercial Implementations**: Block Chain as a Service from
  - IBM
  - Microsoft Azure
  - SAP
  - Deloitte

©2017 Raj Jain

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 3.0 allow sophisticated contracts making it useful for many network and security 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

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 Capital

Scan This to Download These Slides

Raj Jain

http://rajjain.com