Extending Blockchains for Risk Management and Decision Making

Raj Jain
Barbara J. and Jerome R. Cox, Jr. Professor
of Computer Science and Engineering,
Washington University in Saint Louis
Saint Louis, MO 63130 USA
Jain@wustl.edu

Innovation and Breakthrough Forum 2018

Hong Kong, Nov. 9, 2018

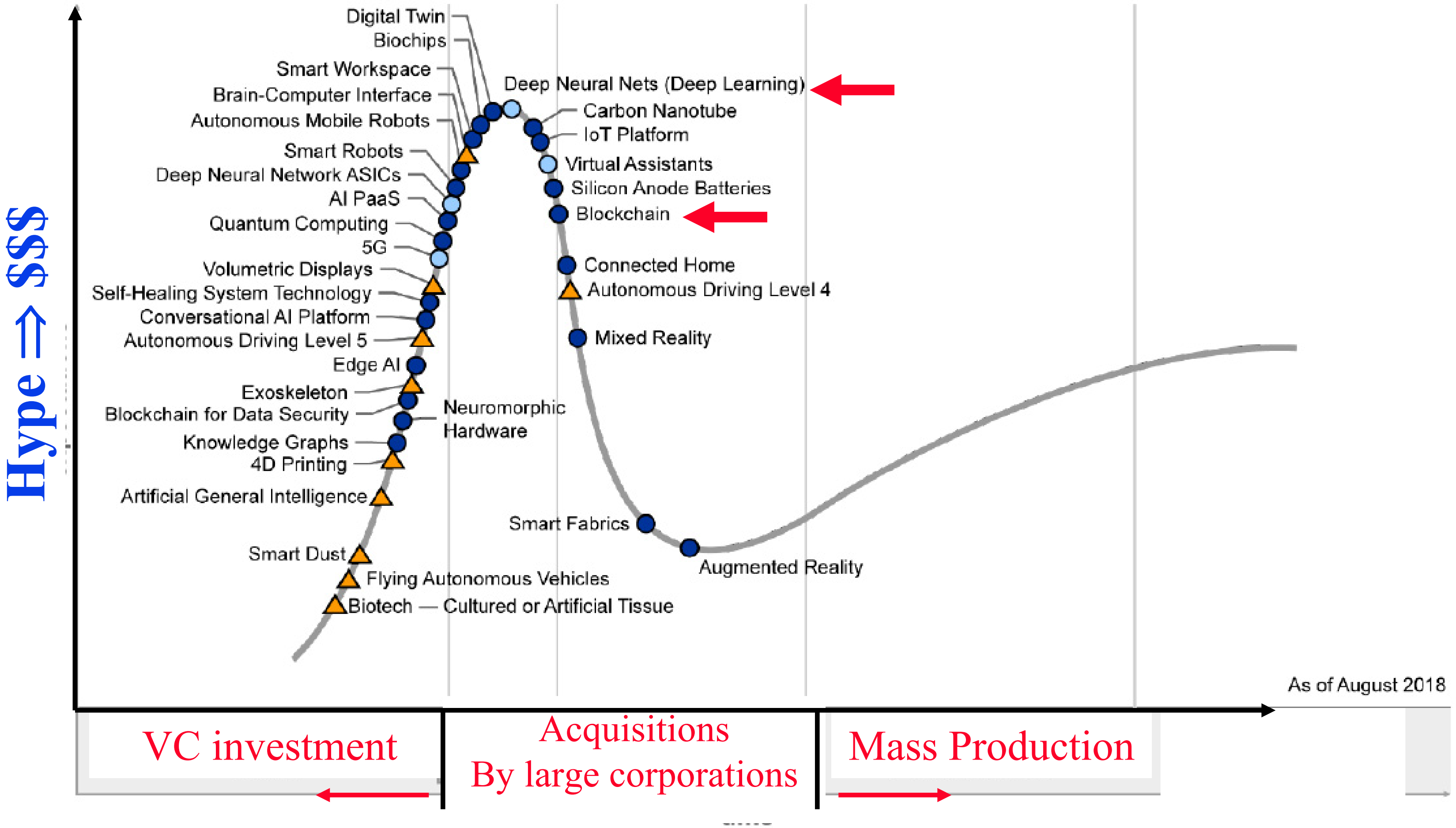
Audio/Video recordings of this talk are available at:

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

Overview

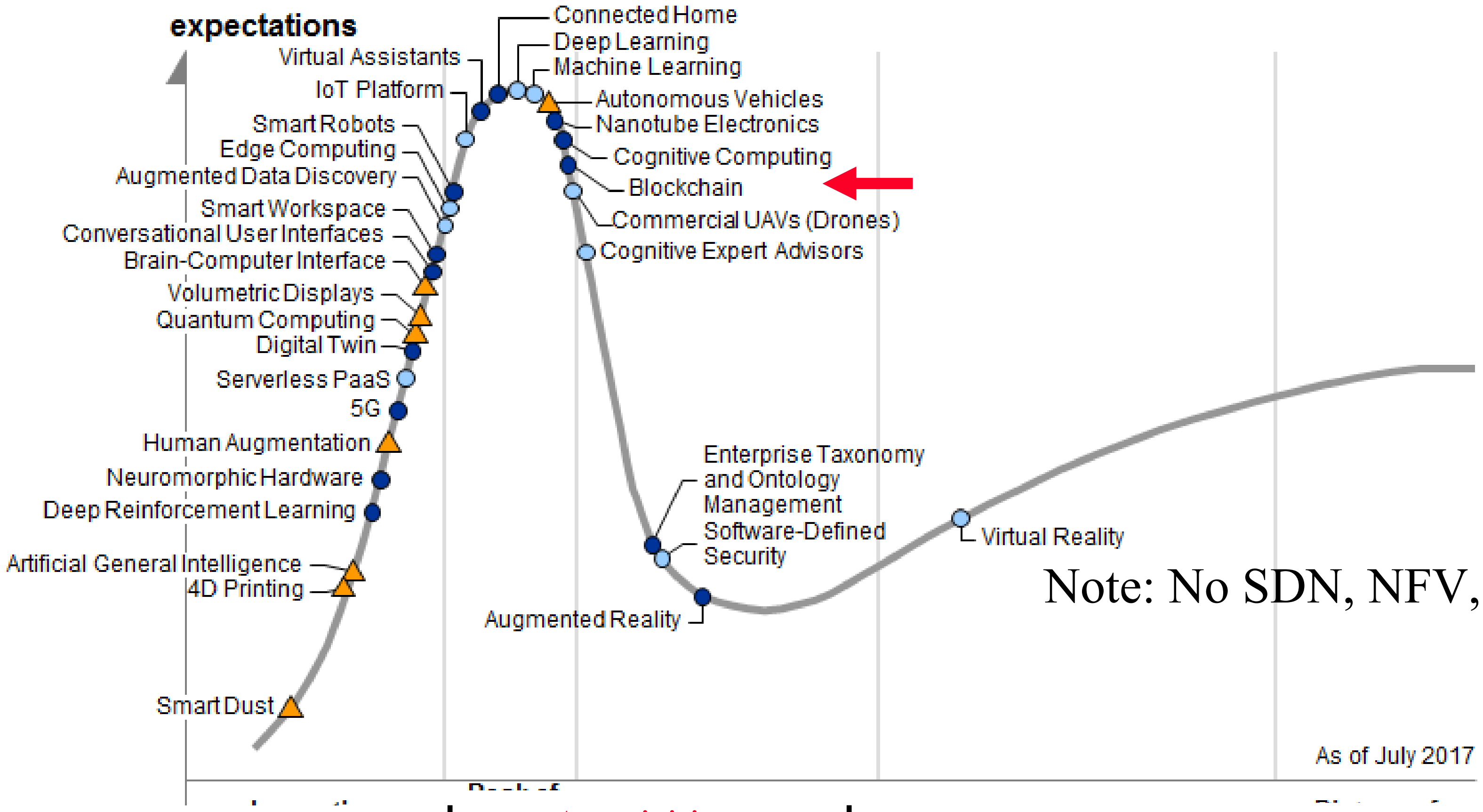
1. Should we invest in blockchain technology?
2. Strengths and weaknesses of the current blockchains
3. Blockchain extension:
   Decision making by converting data to knowledge
4. Empirical feasibility study

Gartner's Hype Cycle For Emering Tech 2018



Ref: M. Walker, "Hype Cycle for Emerging Technologies, 2018," Gartner Report G00340159, 6 Aug. 2018, 73 pp.

Gartner's Hype Cycle For Emering Tech 2017



Note: No SDN, NFV, …

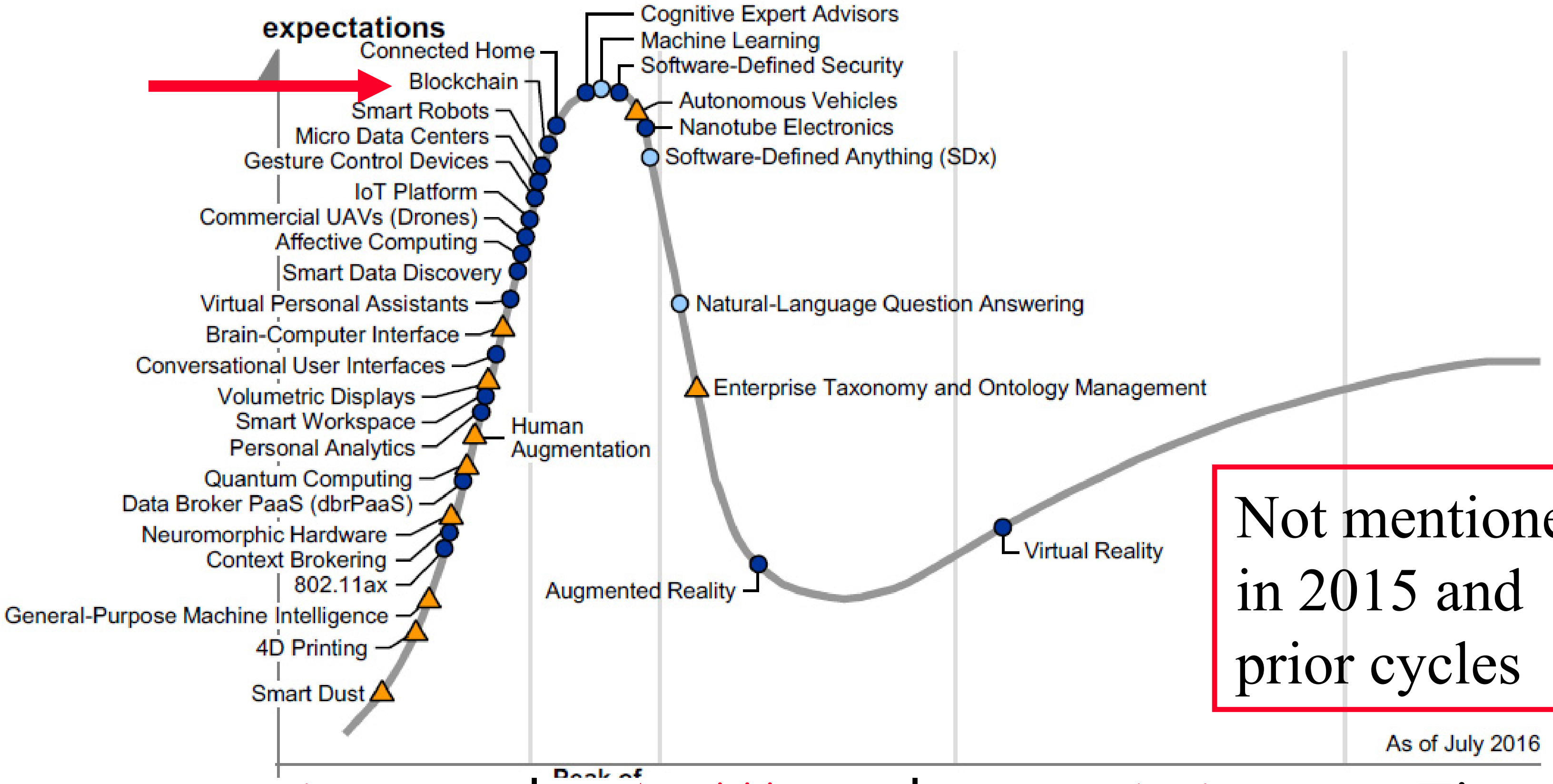
VC investment

Acquisitions
By large corporations

Mass Production

Ref: Gartner, "Hype Cycle for Emerging Technologies, 2017," July 2017, [subscribers only]

Gartner's Hype Cycle For Emering Tech 2016



Not mentioned in 2015 and prior cycles

VC investment

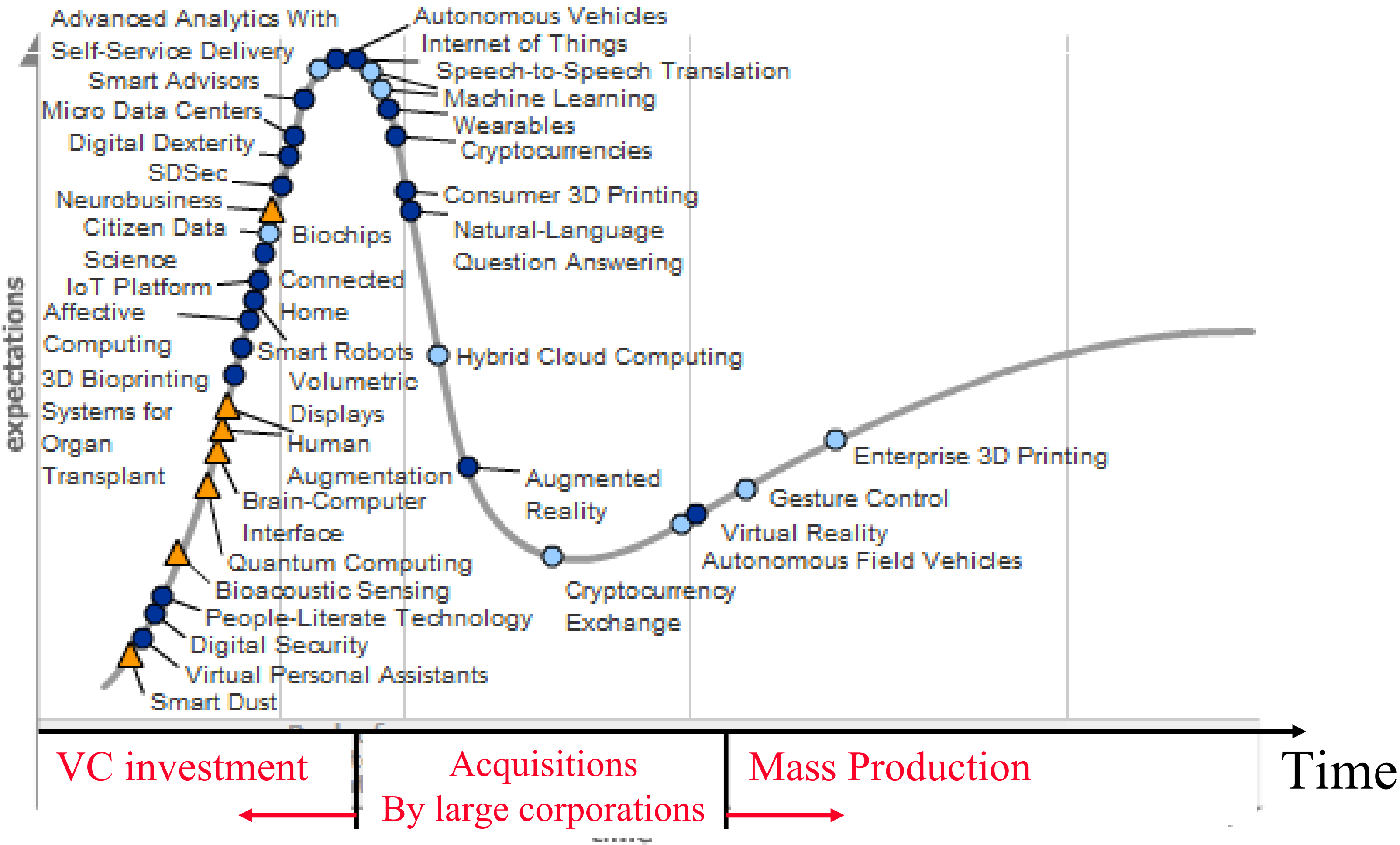
Acquisitions By large corporations

Mass Production

Time

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

Gartner's Hype Cycle For Emering Tech 2015



VC investment

Acquisitions
By large corporations

Mass Production

Time

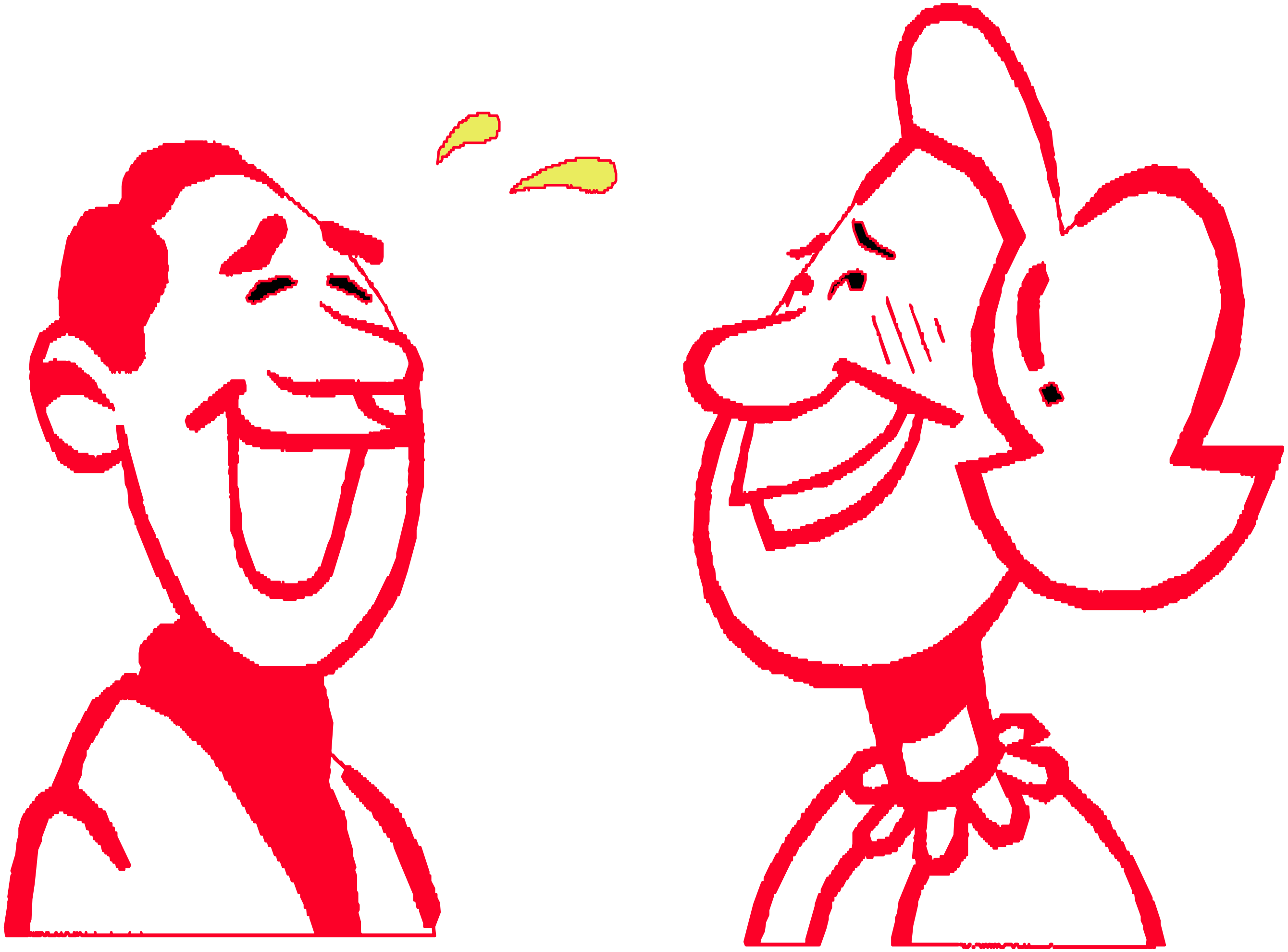
Ref: Gartner, "Hype Cycle for Emerging Technologies, 2015," July 2015, [Available to subscribers only], http://www.gartner.com/document/3100227?ref=QuickSearch&sthkw=hype%20cycle%202015&refval=156919648&qid=fe61993355944ace1c8c01ec2df676d9

Will Blockchain Succeed?

- Blockchain is near the top of hype
- Other examples of hype:
  - Personal Computer 1981
  - Internet 1994*
  - Y2K 1999
  - Bitcoin 2014
- Ignoring hype can lead to failure
  - DEC ignored the PC market
- Being a leader can change your future if the hype succeeds
  - Cisco
- Betting on false hype can lead to wastage
  - Y2K

*Ref: Clifford Stoll, "Silicon Snake Oil: Second Thoughts on Information Highway," Anchor, 1996, 256 pp.

Before



After

Networking: Failures vs Successes

- 1980: Broadband Ethernet 10Broad36 (vs. baseband)
- 1984: ISDN (vs. Modems)
- 1986: MAP/TOP or Token Bus (vs Ethernet)
- 1988: OSI (vs. TCP/IP)
- 1991: DQDB
- 1992: XTP (vs. TCP)
- 1994: CMIP (vs. SNMP)
- 1995: FDDI (vs. Ethernet)
- 1996: 100BASE-VG or AnyLan (vs. Ethernet)
- 1997: ATM to Desktop (vs. Ethernet)
- 1998: ATM Switches (vs. IP routers)
- 1998: MPOA (vs. MPLS)
- 1999: Token Rings (vs. Ethernet)
- 2003: HomeRF (vs. WiFi)
- 2007: Resilient Packet Ring (vs. Carrier Ethernet)
- QoS, Mobile IP, IP Multicast, IntServ, DiffServ, …

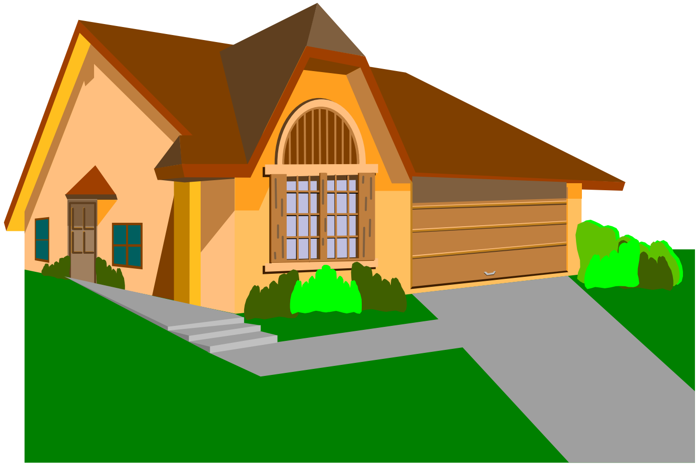
Technology alone does not mean success.

Requirements for Technology Success

1. Low Cost: Low startup cost
   ⇒ Each customer must save.
   2x cost ⇒ 10x performance
2. Killer Application (Crypto)
3. Coexistence with legacy (Current FinTech)
   Existing infrastructure is more important
   than new technology ⇒ Evolution
4. Timely completion
5. Promised Performance (PoW)
6. Manageability
7. Interoperability

Transition strategy is very important

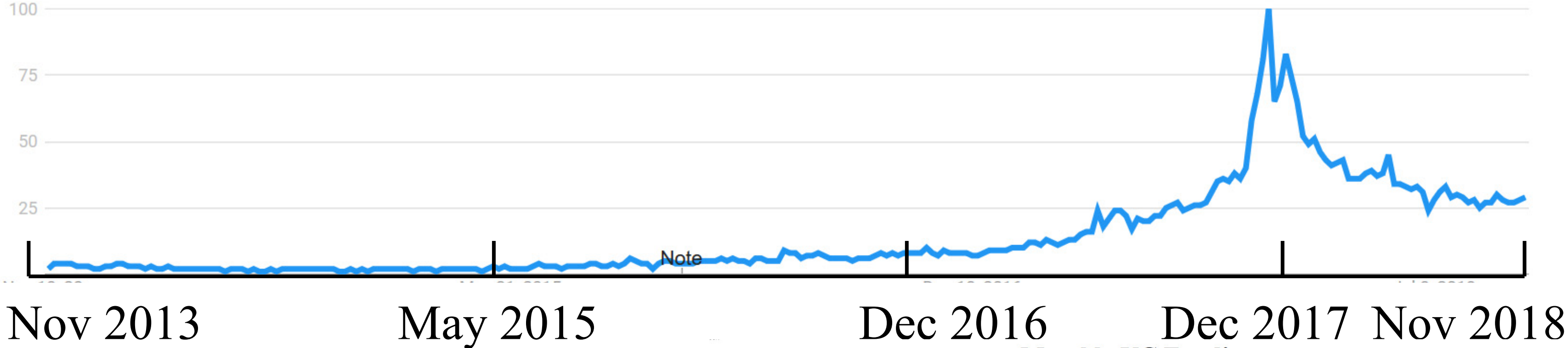
Old House vs. New House

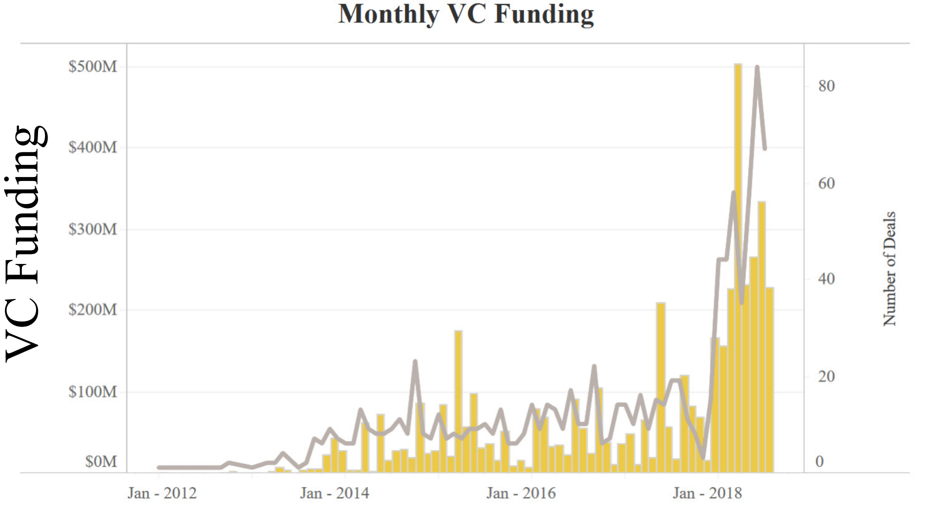


- New needs:
  Solution 1: Fix the old house
  Solution 2: Buy a new house
  Changing millions of houses is difficult.

Given the current state of FinTech, clean slate is difficult

Google Trend: Blockchains





- ❑ 101 pages full of books on Blockchain on Amazon
- ❑ $3.9 B VC investments in 2018 so far
- ❑ $6.3 B in ICO's in 2018

Ref: https://cointelegraph.com/news/venture-capital-investment-in-blockchain-and-crypto-up-280-in-2018-report-shows
https://www.coindesk.com/bitcoin-venture-capital/
https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/

Strengths of Blockchains

1. Decentralized ⇒ No single point of failure/attack
2. No trust assumed among the nodes
   ⇒ Decentralized consensus
3. Cryptographic Security
4. Non-Repudiation guarantee

Can the Blockchains be Enhanced?

Limitation 1: Only facts are recorded

- ❑ Alice is married to Bob
- ❑ Alice gave 20 coins to Bob
- ❑ Alice signed a contract with Bob to pay 10 coins on the delivery of 1 kg of xx.

Limitation 2: Binary Validity

- ❑ All transactions/contracts recorded on the blocks that are committed are valid
- ❑ Those not on the committed blocks and old are invalid
- ❑ So the recording is binary: only 0 or 1.

Limitation 3: Deterministic Events only

- ❑ Can not record that I am only 90% sure that Alice gave 20 coins to Bob.

Ideas to Enhance Blockchains

- Blockchain is just a distributed **data storage** of valid transactions
- All transactions are ***deterministic***
- What's Wrong?
  - Need to convert data to knowledge
  - We are in big data and machine learning age
  - Real life is probabilistic
  - Most to the decisions we make are probabilistic ⇒ All decisions have some risk

Risk Propels Progress

- ❑ Banks take money from risk-averse savers and give them interest
- ❑ Banks invest the money in corporations
  ⇒ Takes the country forward
- ❑ Venture capitalists take risk by investing in half-cooked ideas
- ❑ Startups take risk by working in unchartered territories

Decisions with Risk

- Sell insurance
- Buy insurance
- Sell a stock
- Buy a stock
- Download a software application on your computer
- Update Windows
- Marry someone

Example of a Contract: Wedding

Wedding (Cont)

- ❑ Centralized
- ❑ Decentralized

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

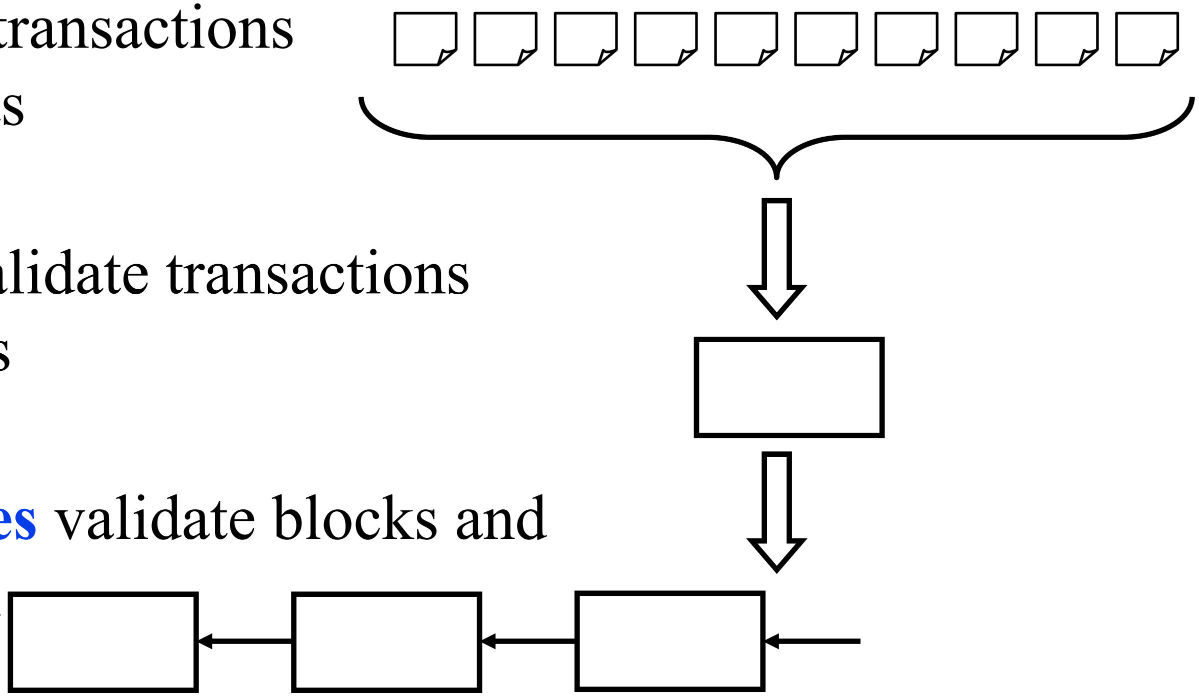
- ❑ Decentralized
- ❑ No single point of failure
- ❑ Very difficult to hack

Current Blockchain Process

1. **Users** broadcast transactions or smart contracts

2. **Mining nodes** validate transactions and create blocks

3. **Blockchain nodes** validate blocks and construct a chain



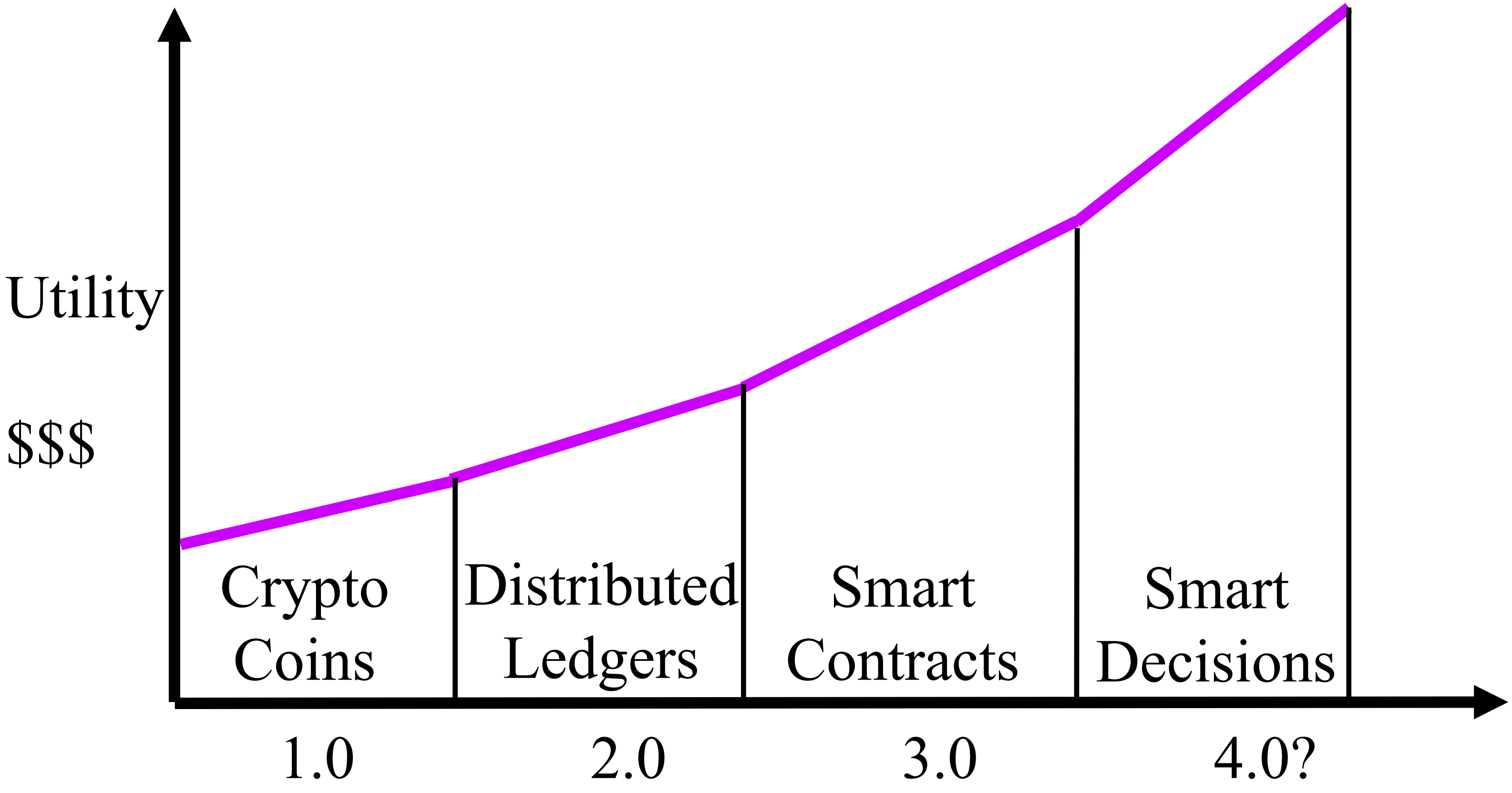
- There are many users, many mining nodes, and many blockchain nodes.
- More nodes ⇒ Better. Less ⇒ Blockchain not required/useful.

Our Goal

- Moving the chain from deterministic to probabilistic
- Moving the chain from storage to computation
- Moving the chain from data to knowledge
- Moving the chain from information to decision making

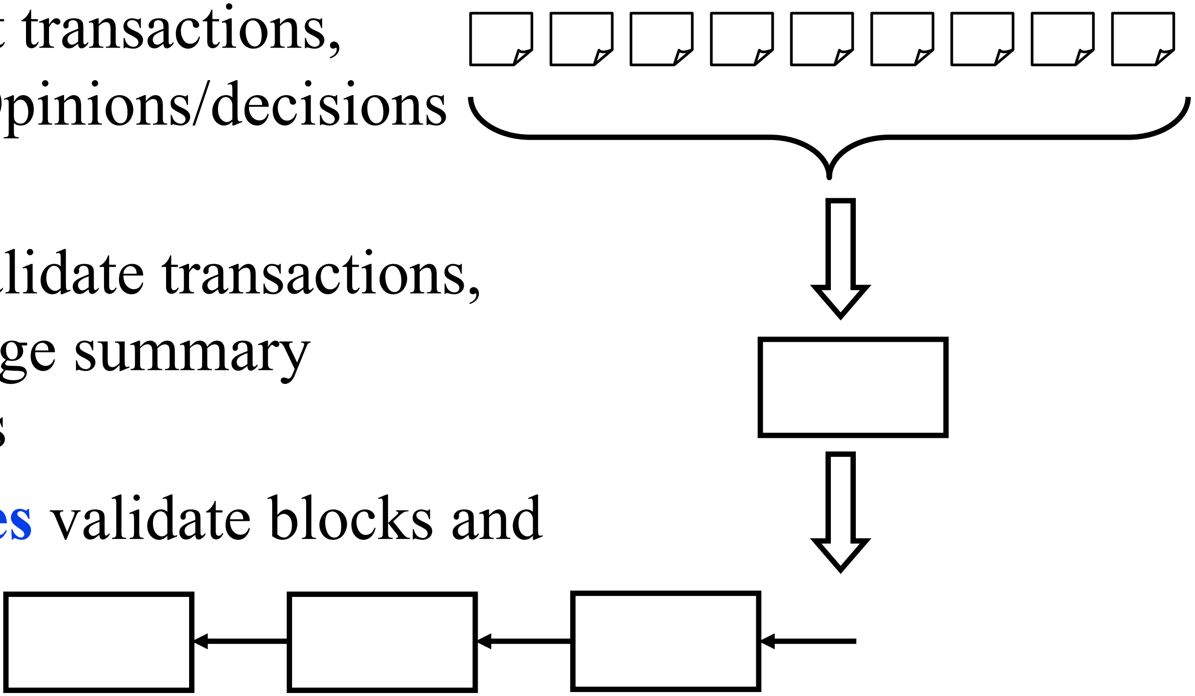
- Google is moving from "Search" to "Suggest" using AI
- A blockchain that provides knowledge
  – A knowledge chain would be more useful

Blockchain Generations



Probabilistic Blockchain Process

1. **Agents** broadcast transactions,
   Transactions = Opinions/decisions
2. **Mining nodes** validate transactions,
   create a knowledge summary
   and create blocks
3. **Blockchain nodes** validate blocks and
   construct a chain



- Two types of users:
  - **Agent nodes** provide their probabilistic decisions
  - **Management nodes** that inquire the blockchain and use it for group decisions

Probabilistic Blockchain Example

- **Issue**: Whether IBM stock will go up tomorrow?
- i^{th} Agent says that the probability that it will go up is p_i
- Summary of all opinions related to this issue is:

  $$\text{P(Stock will rise)} = \text{G}(\{p_1, p_2, \ldots, p_n\})$$

  Here, G is the summarizing function
- In this simple case:

  $$P = \frac{1}{n}\sum p_i$$

- In this example, group decision is the first moment of the individual decisions

Ref: T. Salman, R. Jain, and L. Gupta, "**Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making**," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, Nov. 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

Generalizing the Summary Function

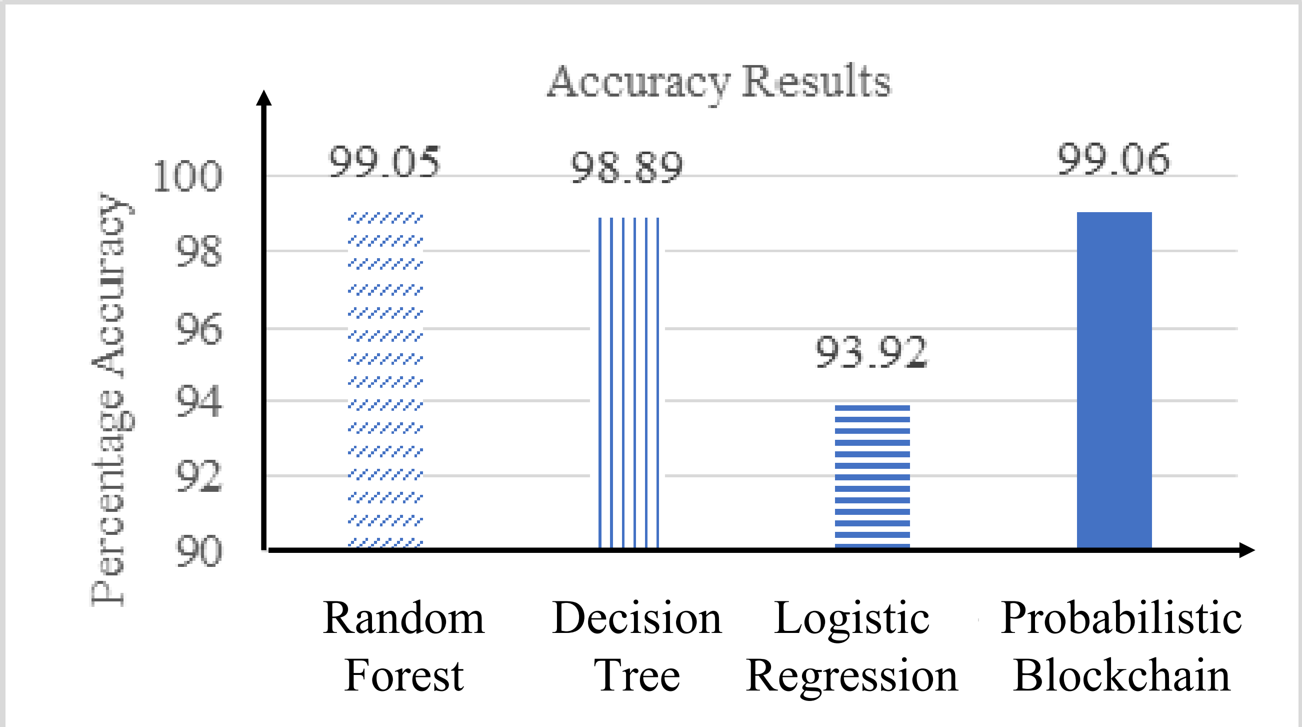
- Summary can be any other reasonable function of individual decisions:
  - 90-percentile
  - Median
  - Mode
  - 2nd Moment
- Summary can be a vector:
  {1st moment, 2nd moment, …, *n*th moment}
- Summary can be the result of any statistical algorithm
- Summary can be the result of a data mining algorithm
- Summary can be the result of a machine learning algorithm

Empirical Validation

- Issue: Whether a network traffic pattern represents intrusion
- 1000 Agents using different machine learning algorithms give their decisions: Yes or No
  - Agents randomly pick one of the 3 algorithms:
    - Random Forest, Decision Tree, Logistic Regression
- Mining nodes summarize these decisions using the majority function

Results

$$\text{Accuracy} = \frac{\text{Correct Predictions}}{\text{Overall Samples}} \times 100\%$$



Distributed decision making is better than any individual decision

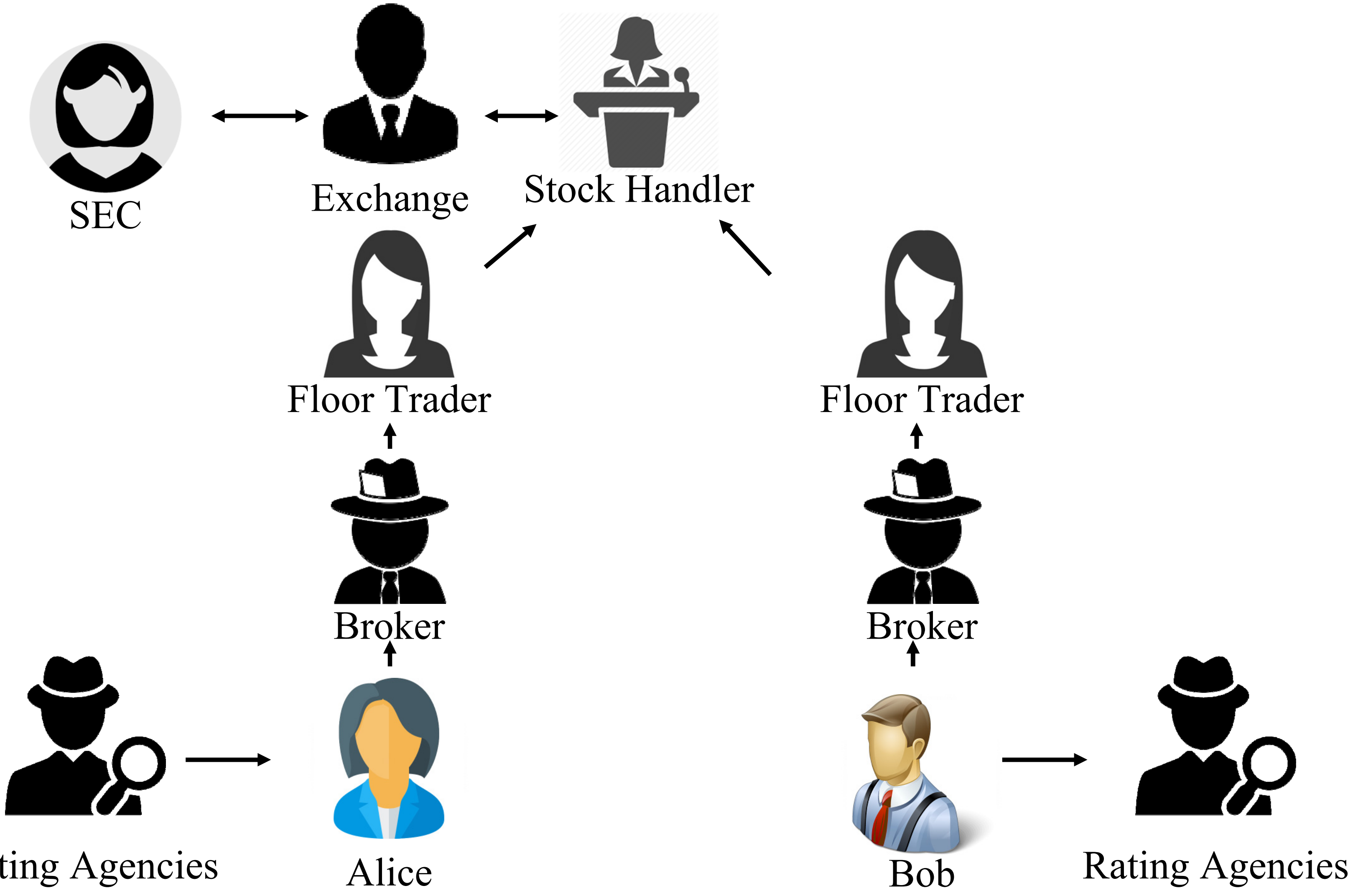
Blockchain 4.0: Database to Knowledge Base

- Blockchain = Distributed database of smart contracts
- Probabilistic blockchain = Knowledge + database
- Database = Who bought, who sold, what quantity, what price, what time
- Knowledge =
  - Where the market is going?
  - Whether we should buy, sell, or hold?

Knowledge Chain

- Customer query to blockchain network:
  How is the IBM stock doing today?
- Blockchain to Customer: The stock is rising with a probability 90%, Confidence 60%, …
- Totally distributed system with no national boundaries, exchange limitations, brokers in between

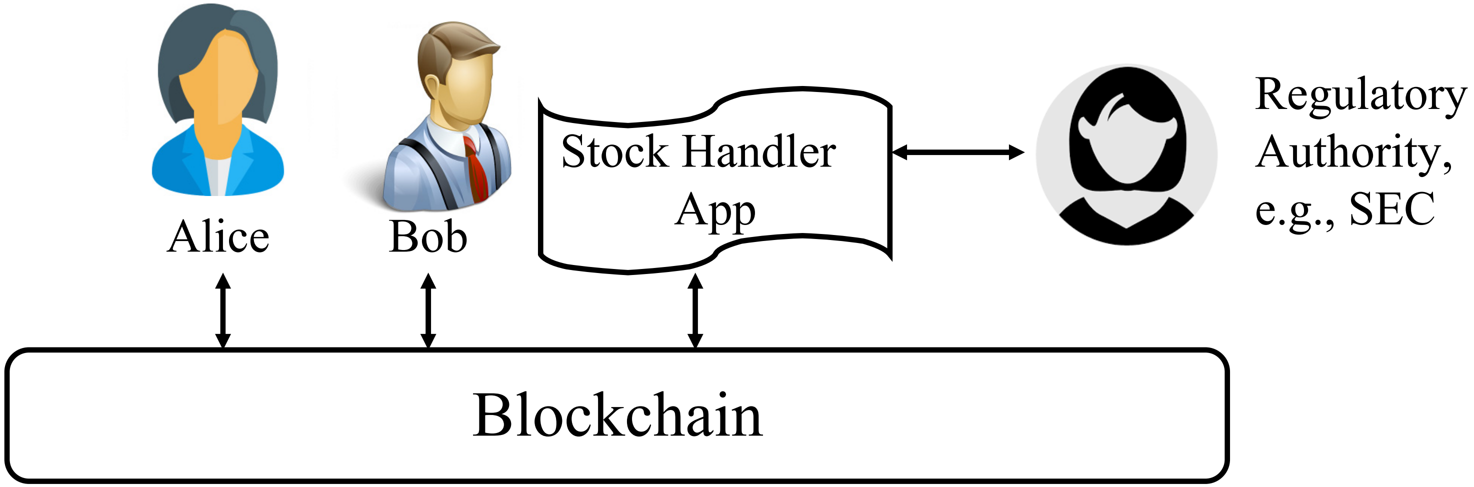
Stock Transactions without Blockchains



Stock Transactions without Blockchains

1. Alice has $10,000 to invest
2. Alice reads reports from **rating agencies**: Morning Star, Ned Davis, Factset, …
3. Alice calls her **broker** Fidelity to buy 10 shares of IBM
4. Fidelity sends the transaction to its **floor trader** in NYSE
5. **Stock Exchange** NYSE ensures that the transaction follows all **SEC** rules
6. Fidelity floor trader makes a bid with IBM **Handler**
7. Bob needs some money
8. Bob reads reports from rating agencies: Morning Star, Ned Davis, Factset
9. Bob calls Schwab to sell 20 shares of IBM
10. Schwab sends the transaction to its floor trader in NYSE
11. NYSE ensures that the transaction follows all SEC rules
12. Schwab floor trader gives the order to IBM handler
13. Handler matches buy and sell orders
14. Handler informs Schwab trader the price and amount
15. Handler informs Fidelity trader the price and amount
16. Fidelity tells Alice the price and the amount after deducting its **commission**
17. Fidelity deducts the amount from Alice's account
18. Schwab tells Bob the price and the amount after deducting its **commission**
19. **Three days** later the money shows up in Bob's account
20. There are many more steps if the transaction crosses the nation boundaries

P2P Stock Transactions with Blockchains



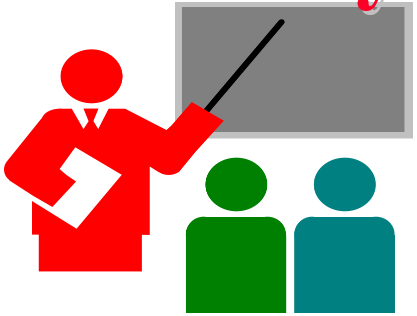
1. Alice submits a smart contract to buy the stock
2. Bob submits a smart contract to sell stock
3. Stock handler app matches the transactions, ensures that it complies with SEC rules and submits a transaction

P2P Stock Transactions Benefits

1. Matching = Computation that can be done inside the blockchain by miners or outside by an application
2. Inside ⇒ In one block time,
   Outside ⇒ a few block time
3. Reduced number of intermediary
   ⇒ Less cost and faster settlement
   ⇒ Increased fairness and transparency

Ref: Blockchain Dude, "The Collision of Stock Exchanges and Blockchain," https://hackernoon.com/the-collision-of-stock-exchanges-and-blockchain-55d222b87a8

Summary



1. Blockchains provide an immutable, secure, distributed database
2. Three generations of blockchains: Crypto currency, Assets, Smart contract
3. All three generations are deterministic and provide storage
4. The next generation needs to connect computation and AI to make knowledge/decisions out of data
5. Consensus can be probabilistic result of any statistical algorithm, data mining, or machine learning

Related Papers

- Tara Salman, Raj Jain, and Lav Gupta, "**Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making**," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, November 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm
- Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka, "**Security Services Using Blockchains:A State of the Art Survey**" IEEE Communications Surveys and Tutorials, Accepted September 2018, 28 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm

Related Talks

- Raj Jain, "**Blockchains: Networking Applications**," An invited talk at the 38th IEEE Sarnoff Symposium, Newark, NJ, Sep 19, 2017, http://www.cse.wustl.edu/~jain/talks/blc_srnf.htm
- Raj Jain, "**Blockchains: The Distributed Trust Technology**," Keynote at The 2017 International Conference on Computer, Information and Telecommunication Systems (CITS 2017), Dalian, China, July 21, 2017, http://www.cse.wustl.edu/~jain/talks/cits17.htm
- Raj Jain, "**Blockchains: The Revolutionary Trust Protocol**," BEL Keynote at 22nd Annual International Conference on Advanced Computing and Communications (ADCOM 2016), Bangaluru, India, Sep 10, 2016, http://www.cse.wustl.edu/~jain/talks/blc_ad16.htm Grand Tara

List of Acronyms

ADCOM	Advanced Computing
AI	Artificial Intelligence
CITS	Computer, Information and Telecommunication Systems
DEC	Digital Equipment Corporation
DNS	Domain Name Service
IBM	International Business Machines
IEEE	Institution of Electrical and Electronics Engineers
ICO	Initial Coin Offering
NFV	Network Function Virtualization
PC	Personal Computer
SDN	Software defined networking
VC	Venture Capitalist

Scan This to Download These Slides

Raj Jain

Jain@acm.org

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