Extending Blockchains Beyond Smart Contracts

Raj Jain
Barbara J. and Jerome R. Cox, Jr. Professor
Washington University in Saint Louis
Jain@wustl.edu

Blockchain Connect Conference, San Francisco, January 11, 2019

Audio recordings of this talk are available at:
http://www.cse.wustl.edu/~jain/talks/pbc_svi.htm

Overview

1. Strengths and weaknesses of the current blockchains
2. Blockchain extension:
   Decision making by converting data to knowledge
3. Empirical feasibility study

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 gave 20 coins to Bob

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
    $\Rightarrow$ 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
  $\Rightarrow$ 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

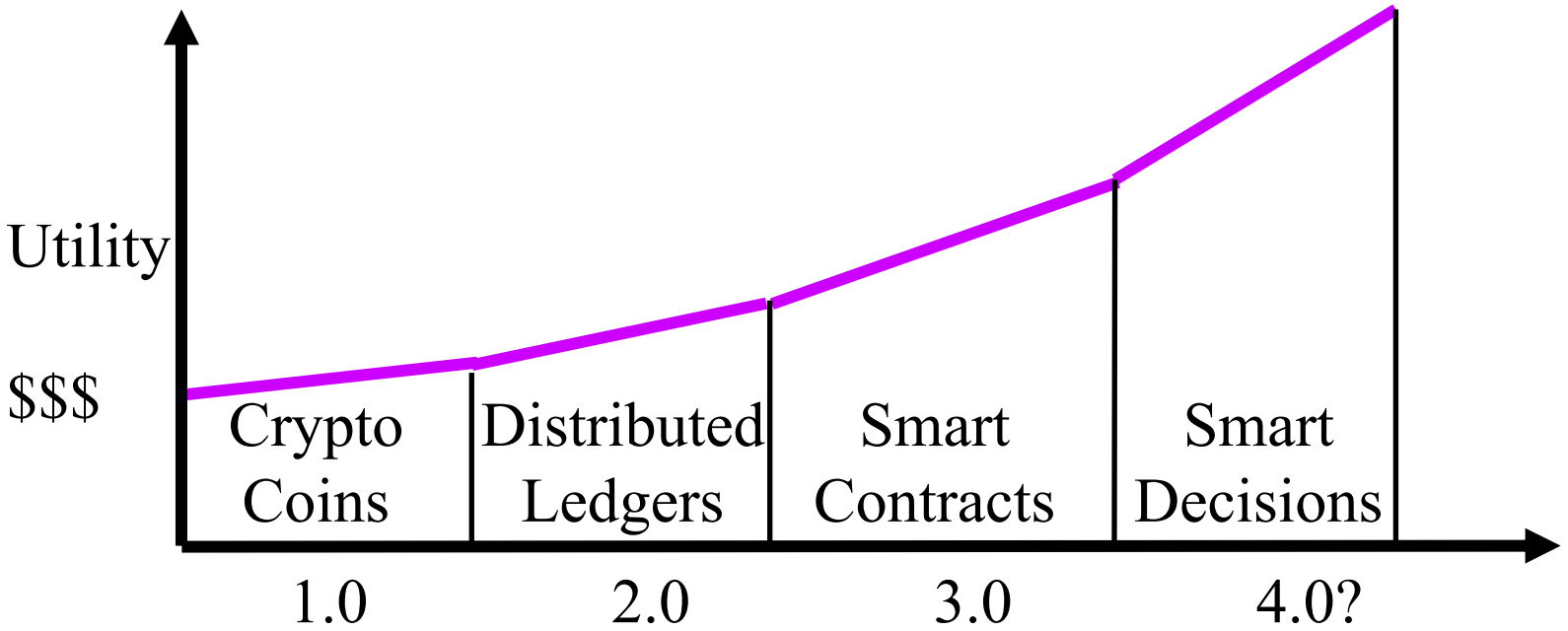
- Sell insurance
- Buy insurance
- Sell a stock
- Buy a stock
- Download a software application on your computer
- Update Windows
- Marry someone

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
- A blockchain that provides knowledge
  – A knowledge chain would be more useful

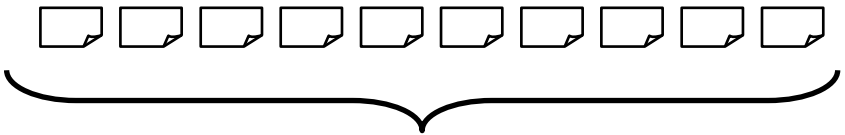
Ref: T. Salman, R. Jain, and L. Gupta, "**Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making**," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, Nov. 8-10, 2018, 9 pp., http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

Blockchain Generations

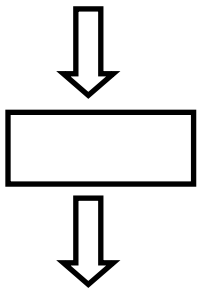


Current Blockchain Process

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



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

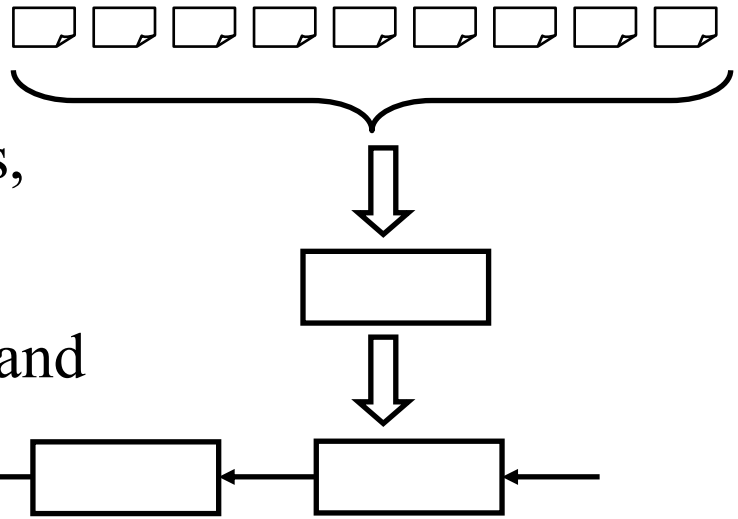


3. **Blockchain nodes** validate blocks and construct a chain

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

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

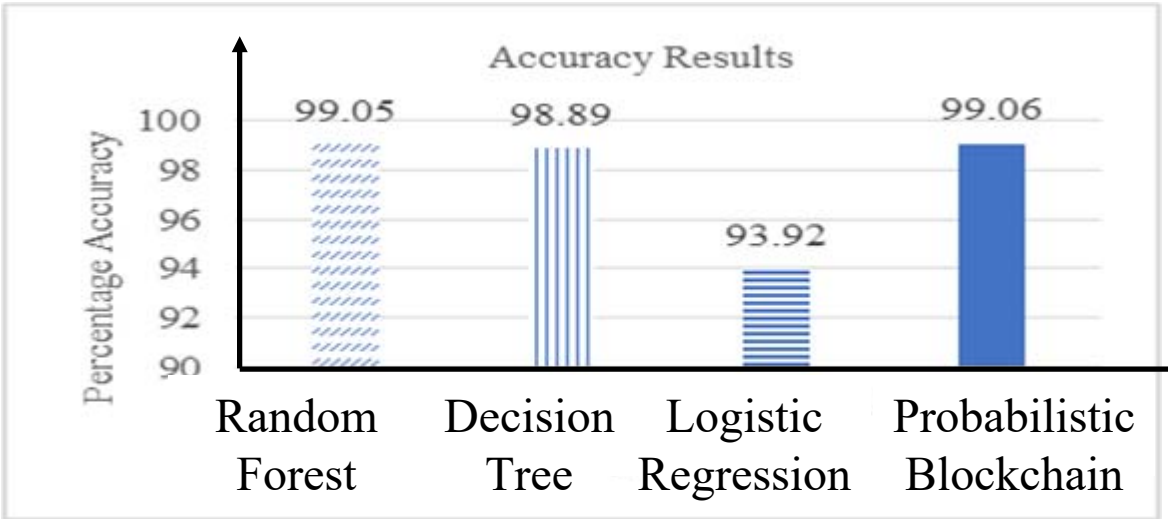


Empirical Validation

- 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

Generalizing the Summary Function

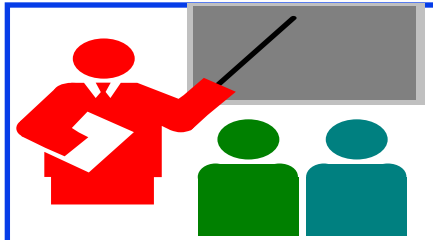
- Summary can be any other reasonable function of individual decisions:
  - 90-percentile
  - Median
  - Mode
  - 2nd Moment
- Summary can be a vector: {1st moment, …, n^{th} moment}
- Summary can be the result of any statistical algorithm
- Summary can be the result of a data mining algorithm
- Summary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

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



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, "**Extending Blockchains for Risk Management and Decision Making**," Invited talk at Innovation and Breakthrough Forum 2018, Hong Kong, Nov. 9, 2018, http://www.cse.wustl.edu/~jain/talks/pbc_ibf.htm
- 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@wustl.edu

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