Introduction to Blockchains for Computer Networking

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/cse570-23/

Student Questions

Overview

1. Trend: Centralized to Decentralized

2. Importance of Blockchain

3. Technical Innovations of Bitcoin

4. Blockchain Applications

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/

Example of a Contract: Wedding

Wedding (Cont)

Centralized

Decentralized

Student Questions

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

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

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

Blockchains

❑ **What** it allows:
  ➢ Two strangers can complete a transaction without a third party
  ➢ 1st Generation: Transaction = Money transaction
  ➢ 2nd Generation: Contracts, Agreements, Property, …
  ➢ Revolutionizing and changing how 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, …

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/   ©2023 Raj Jain

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, etc.)

❑ **Credit Card companies**

❑ In all cases:

1. There is a central third party to be trusted

2. The central party maintains an extensive database of information
   $\Rightarrow$ Attracts Hackers

3. The central party may be hacked
   $\Rightarrow$ affects millions

4. The central party is a single point of failure.
   It can malfunction or be bribed.

Student Questions

Trend: Centralized to Decentralized

❑ **Trend**: Make everything decentralized with no central point of control

❑ You can send money to your friends in Russia and 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 $\Rightarrow$ Fast

   4. No single point of control $\Rightarrow$ No monopoly $\Rightarrow$ Cheaper

❑ Libertarians decided to build a decentralized system with no central authority. Blockchain is one way to do this.

Student Questions

Bitcoin

❑ First Successful Virtual Currency

❑ Has survived 11 years and has become legal in several jurisdictions

❑ 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 = 8473.34 USD (Nov. 17, 2019)
= 66,692.00 USD (Nov. 17, 2021)

❑ 10^{-8} BTC = 1 Satoshi = 0.00008 cents (Nov. 17, 2019)
= 0.00066 cents (Nov. 17, 2021)

❑ 18 Million BTC (Nov. 17, 2019) 18,749,318.75 BTC (Nov. 17, 2021)

❑ A total of 21 Million BTC will be generated.

Student Questions

Bitcoin History

❑ Satoshi Nakamoto published a *whitepaper* in 2008. How to do a direct transfer of money without involving a 3rd party.

❑ He also published a complete reference code to transact, store, and mint Bitcoins. Made the software open source.

❑ He supported the software and answered all questions for three years and then disappeared
(maybe 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

Student Questions

❑ This is true technically about Proof of Work, but isn't it called PoW because of the mathematical puzzle to mine a block and not necessarily having a majority?

The ability to solve a puzzle quickly ensures that more miners will follow your block in the future => Majority of miners.

❑ Can you explain Proof of Stake, if possible? I've heard some crypto is embracing PoS to reduce computation expenditure.

Stake = Investment
Whoever owns the highest number of bitcoins wins the lottery. (Capitalism). No puzzle-solving is required. Ether has recently adopted PoS.

Hash Function

- Hash tables used in data searches
- The hash function should
- Take variable size input
- Produce fixed output size (Size of the table)
- Be easy to compute
- Be pseudorandom so that it distributes uniformly over the table $\Rightarrow$ Minimizes collisions
- Deterministic: The same input always produces the same hash
- Example: h(M) = M mod 9; M=13 $\Rightarrow$ h(M)=4
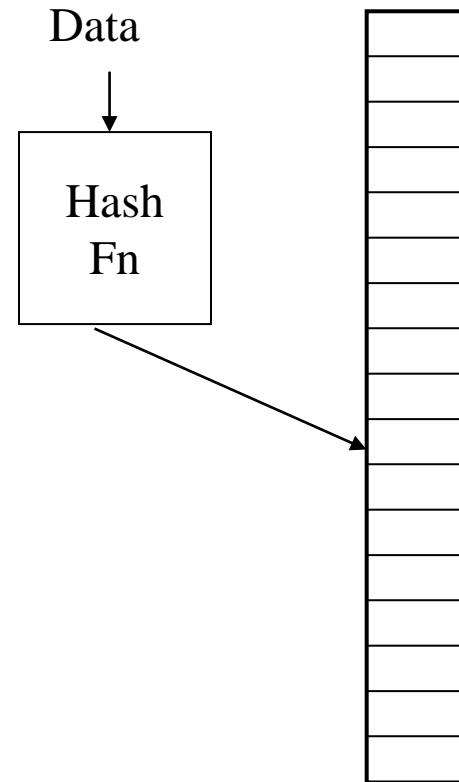
Data

Hash Fn

Cryptographic Hash Functions

❑ One-way
It is not possible to find any M, given h.

❑ Very Very difficult to compute M given h(M)

❑ SHA-2: Secure Hash Algorithm standardized by the National Institute of Standards and Technology (NIST).

➢ SHA-256 produces a 256-bit hash of any number

❑ RIPEMD: RACE Integrity Primitive Evaluation developed in the EU

➢ RIPEMD160 produces a 160-bit hash

Student Questions

❑ Are SHA-2 and SHA256 the same? Or is it that SHA-2 has variable length options, and one can be 256 bits?

SHA-2 is the 2nd version of SHA. All versions are used with different key lengths. Users indicate their key length after SHA. So, SHA-256 is SHA with a 256-bit key. There is clarity since version numbers are 1, 2, or 3. Keys are 512+.

Secret Key Cryptography

❑ Secret Key Cryptography:

Plain Text $\longrightarrow$ Encrypted Text
Key

Encrypted Text $\longrightarrow$ Plain Text
Key
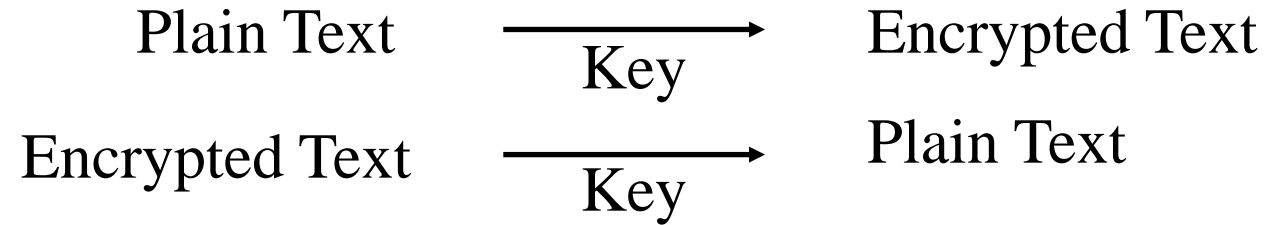
❑ The key must be kept secret.
Anyone with the key can read/write/change messages.

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

Public Key Encryption

❑ Invented in 1975 by Diffie and Hellman at Stanford

❑ Encrypted_Message = Encrypt(Key1, Message)

❑ Message = Decrypt(Key2, Encrypted_Message)

❑ Keys are **interchangeable**:

❑ One key is made **public,** while the other is kept **private**

❑ Sender knows only the public key of the receiver ⇒ **Asymmetric**

Ref: http://en.wikipedia.org/wiki/Public-key_cryptography

Student Questions

❑ Do all encryption actions in blockchains use public keys?

Yes, for public blockchains. There can always be exceptions in private blockchains.

Public-Key Authentication and Secrecy

B's Public Key	A's Private Key	Message

A ──▶ B
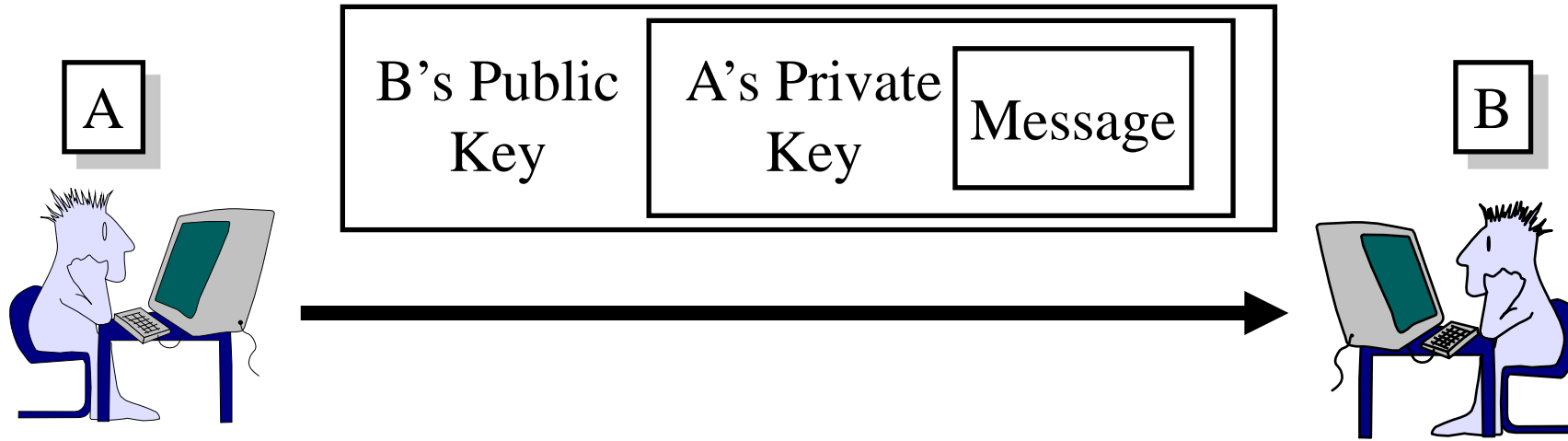
□ A encrypts the message with its private key and then with B's public key

□ B can decrypt it with its private key and A's public key

□ No one else can decrypt ⇒ Secrecy

□ No one else can send such a message
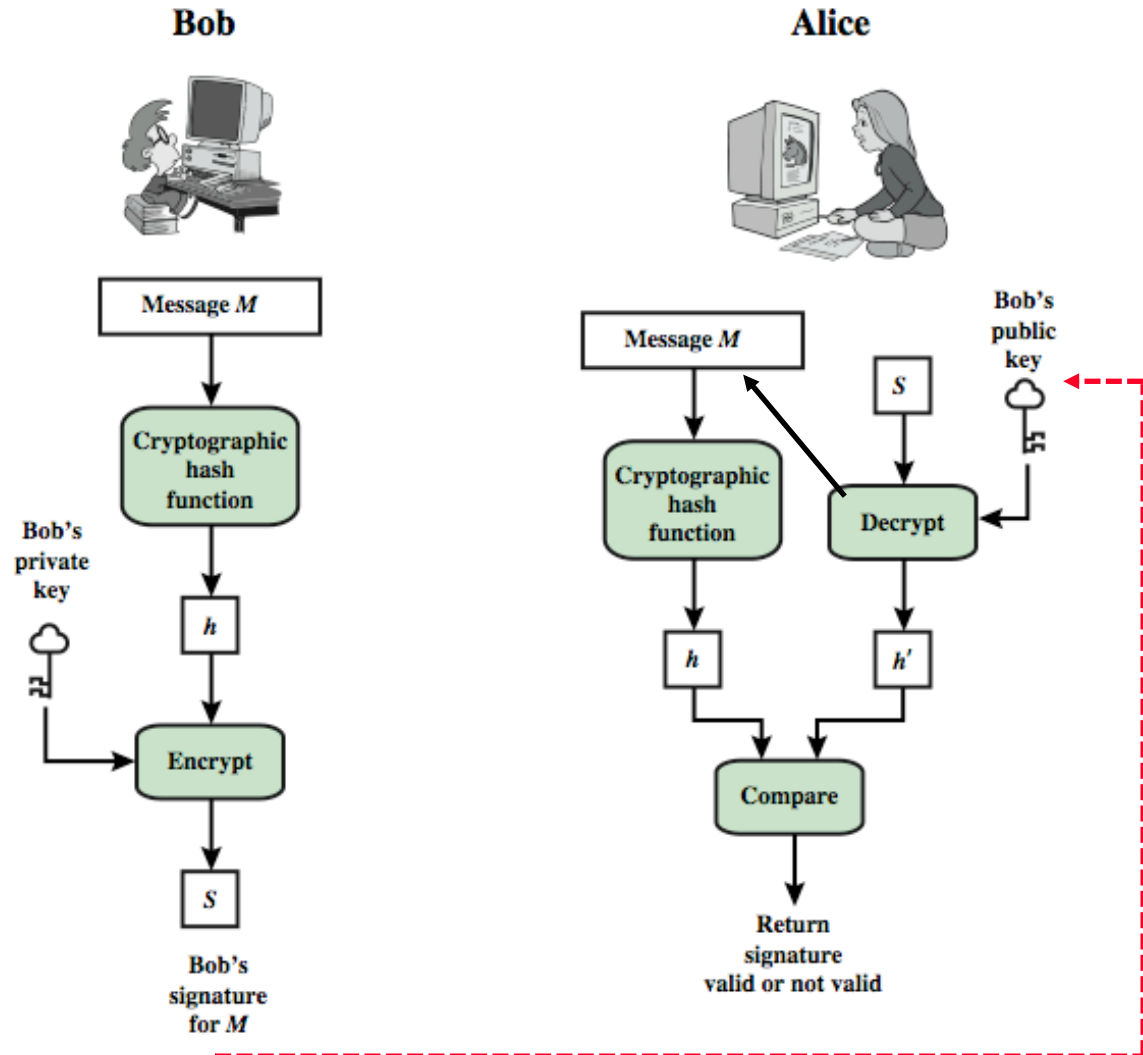⇒ B is assured that the message was sent by A
⇒ Authentication

Digital Signature

Bob

Message M → Cryptographic hash function → h → Encrypt → S (Bob's signature for M)

Bob's private key → Encrypt

Alice

Message M → Cryptographic hash function → h → Compare

S → Decrypt → h' → Compare

Bob's public key → Decrypt

Compare → Return signature valid or not valid

❑ The figure on the left explains the sending process, whereas the right figure is for the receiver side. Correct?
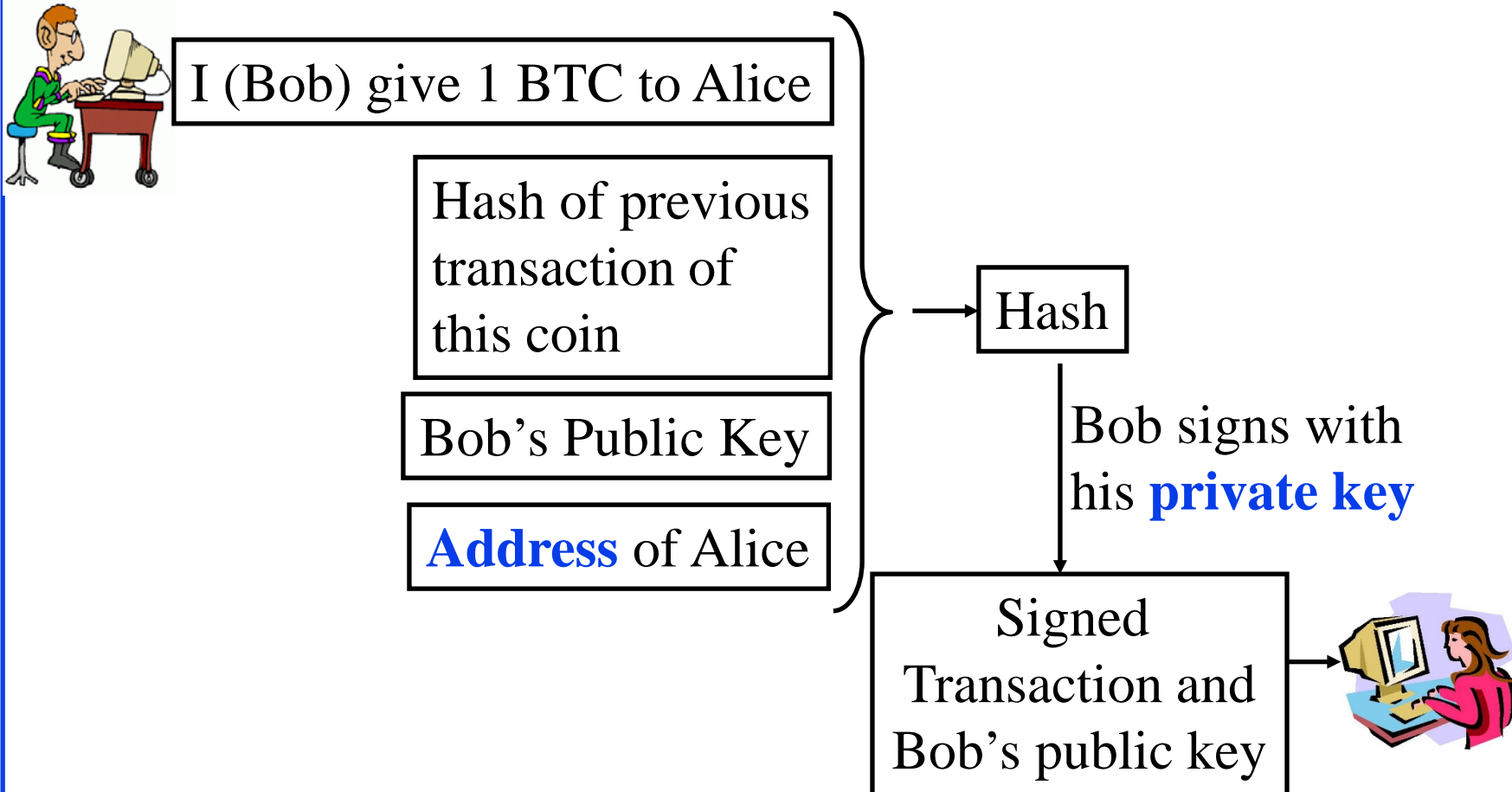
Yes.

❑ To double confirm, does Hashing the msg have nothing to do with signing? It is just for the msg integrity but not for authenticating the sender? as digital signature is purely related to public-key cryptography.

Hashing the message is required for signing. The signature length is equal to the size of the item being signed. Hashing reduces the length of the signature. Otherwise, the signature would be the same length as the message.

http://www.cse.wustl.edu/~jain/cse570-23/
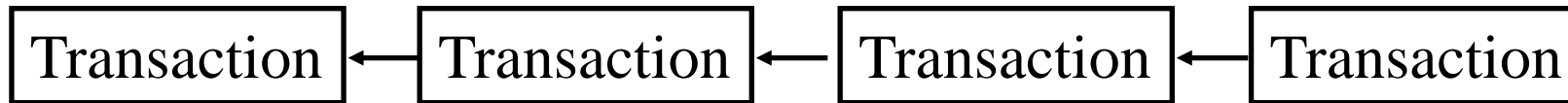
©2023 Raj Jain

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

Blocks

❑ Transaction Chain:

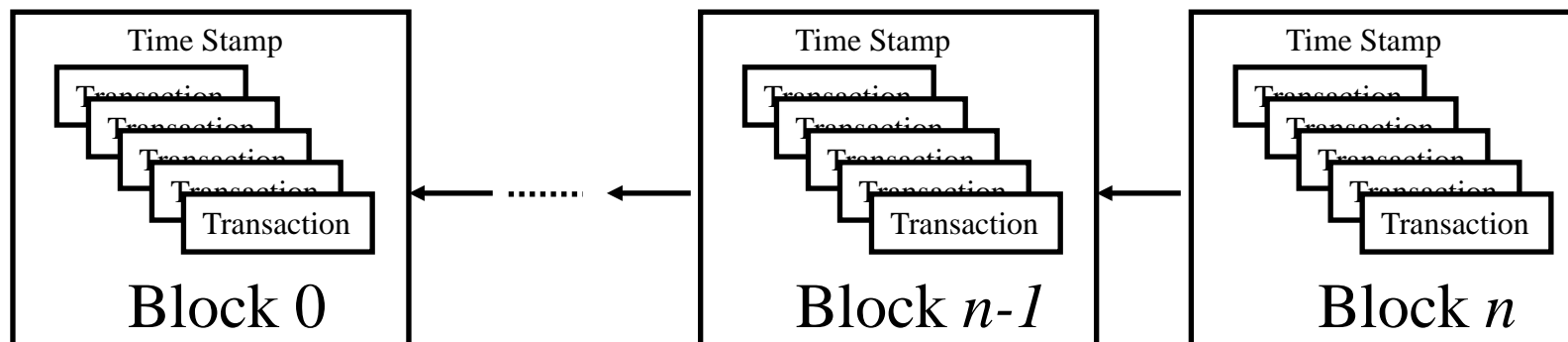| Transaction | ← | Transaction | ← | Transaction | ← | Transaction |

❑ 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

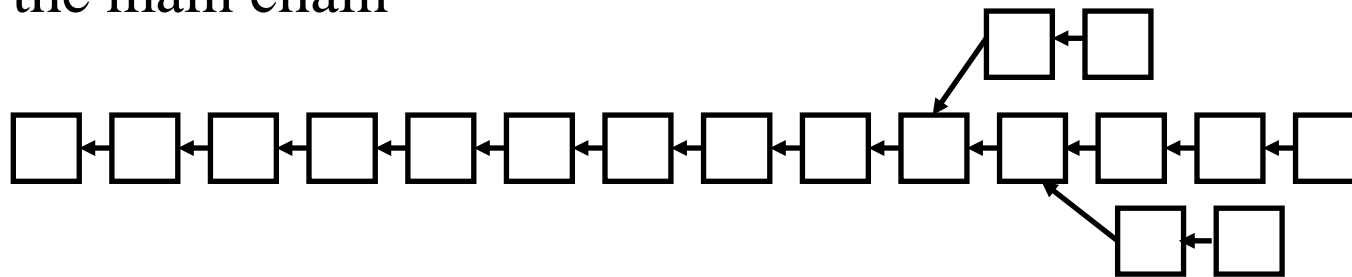Time Stamp
Transaction
Transaction
Transaction
Transaction
Transaction
Block 0

← .... ←

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
- The miner with the highest computer power v
  Their block is added to the end of the chain
- Miner is rewarded.
  They are allowed to mint a few new coins and keep them
- Proof of computing power ⇒ **Proof of work**
  ⇒ Solve a puzzle
- The 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 lowercase – 4 (0, O, 1, I)
that is, lowercase L and uppercase 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 one 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

❑ RIPMD160 of 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

Student Questions

❑ Bitcoin belongs to the blockchain. The blockchain is a decentralized database. What principle is Bitcoin based on encrypting and sorting the database? Why is he so difficult to track?

Physical ID to Public address is not known.
Þ Anonymous

Proof-of-Work (PoW)

❑ When someone requests a service, ask them to do something difficult for the requester but easy to verify for the server. Captcha is one example

❑ Bitcoin requires 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 more challenging as the computing power increases with Moore's Law.
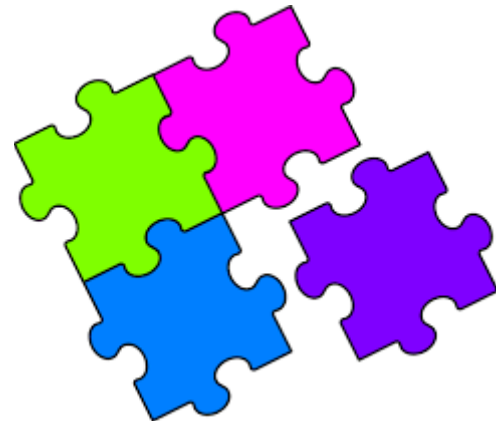
Puzzle

❑ Find a nonce that will make the hash of the block header less than a specified target

❑ Lower target $\Rightarrow$ More challenging to find

❑ A puzzle can be made harder/easier by specifying a higher or lower target

❑ Target is adjusted by all miners every two weeks (2016 blocks), so it takes 10 minutes to solve the puzzle.

$$+2^{256}-1$$

← Target or difficulty

| Block Header ‖ Nonce | → | Hash | →

0

http://www.cse.wustl.edu/~jain/cse570-23/   ©2023 Raj Jain
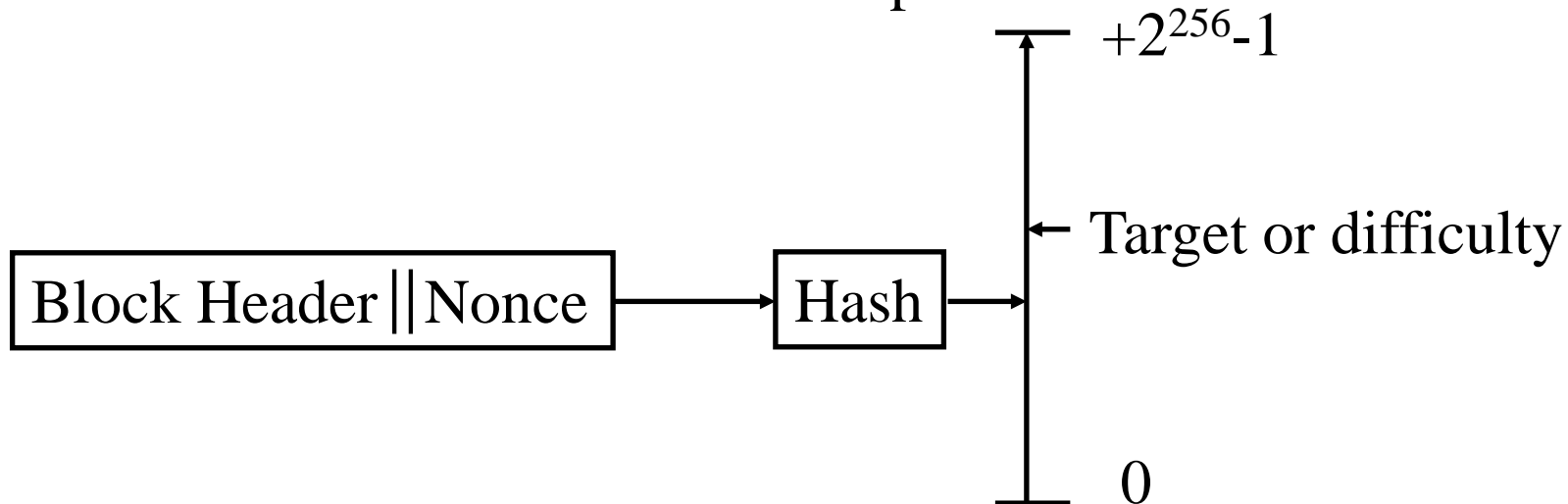
Block Structure

❑ 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, difficulty, nonce

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

Transactions

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

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain
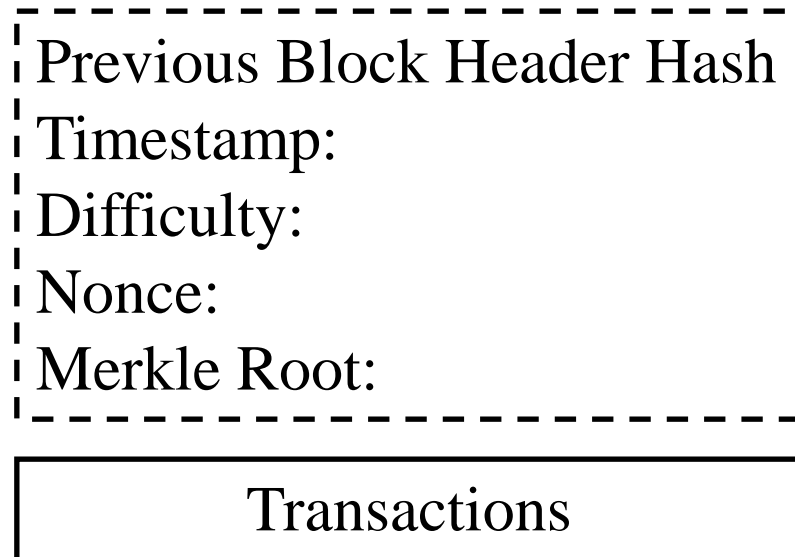
Student Questions

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 the hash of the concatenation of children
- ❑ Takes $\log_2(n)$ comparisons to find the transaction among n
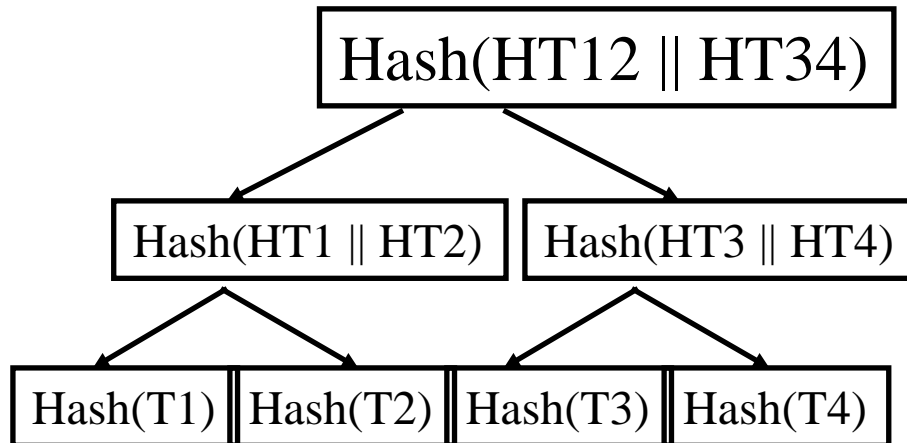
Ref: A. M. Antonopoulos, "Mastering Bitcoin," O'Reilly, 2015, 274 pp.

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
$\Rightarrow$ 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 licenses, 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

Student Questions

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

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

17.26

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

Student Questions

> Explore blockchains for multi-domain/centralized systems

Networking Applications (Cont)

❑ **NameCoin**: A decentralized key-value registration and transfer platform using blockchains.

   ➢ A decentralized **Domain Names Registry**

   ➢ .bit domain names

Student Questions

Ref: T. Salman, et al, "**Security Services Using Blockchains:A State of the Art Survey**" IEEE Communications Surveys and Tutorials, First Quarter 2019, Volume 21, Issue 1, 858-880 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm
http://www.cse.wustl.edu/~jain/cse570-23/

Washington University in St. Louis

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

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

Data Provenance

❑ Keeping track of the origin and history of the 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

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/   ©2023 Raj Jain

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 the rights to all personal information?

- Can the user hide their 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

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/

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

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

Blockchain Challenges

- **Selfish mining**: Someone creating a large number of bad blocks, keeping the validators busy with discards

- **Sybil Attacks**: Someone 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

Student Questions

- What would be the incentive for selfish mining? i.e., what can the attack gain from generating bad blocks except for wasting miners' time and computing resources? *This is a "Denial of Service (DoS)" attack. Busy validators may not get some good blocks in time.*

- Can 51% of attacks tamper with the content on the previous blocks? *No one can change previous blocks.*

- Is it possible to implement a 51% attack? Is it possible to gather computing power? Even if computers are gathered together, does the computing power increase linearly? *It is almost happening. Three mining pools in China were all that were left recently.*

- *You mentioned that the Bitcoin blockchain is centralized even if designed to be distributed. Is that because some people have much work proof? It has become centralized in practice because some pools have too much computing power dedicated to mining.*

http://www.cse.wustl.edu/~jain/cse570-23/   ©2023 Raj Jain

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 $\Rightarrow$ More random

❑ **Proof of Importance**

❑ **Proof of Stake**

Student Questions

❑ Could you explain how Proof of Stake works? Proof of Work makes sense to me, and how it is used in Bitcoin mining, but I can't see how Proof of Stake would work for Ethereum.

You need to invest in the currency to be eligible to mine it. There are many variations.

❑ How do we verify proof of space? If someone claims to have it? Doesn't this method also have an electricity problem, similar to the proof of work? What is the main advantage of using proof of importance over proof of stake? And vice versa?

These questions are irrelevant to us since we do not use them.

❑ Are there any proposed solutions for communication overhead? *No.*

Blockchain Implementations

□ **Open Source Implementations**:
  ➢ Bitcoin
  ➢ Ethereum
  ➢ Hyperledger

□ **Commercial Implementations**: Block Chain as a Service from
  ➢ IBM
  ➢ Microsoft Azure
  ➢ SAP
  ➢ Deloitte

Student Questions

# Key Strengths of Blockchains

1. **Distributed**: No single point of failure

2. **Decentralized Consensus**: Transactions are valid only if agreed upon by the majority

3. **Trustless**: Transacting or processing parties do not need to trust

4. **Cryptographic Security**: Elliptic Curve Cryptography

5. **Non-Repudiation Guarantee**: All transactions are signed

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

  ➢ Real life is probabilistic

  ➢ Most decisions we make are probabilistic
    ⇒ All decisions have some risk
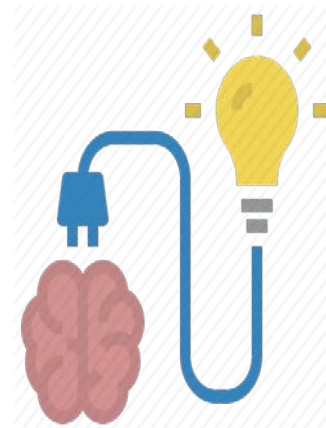
http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

Risk Propels Progress

❑ Banks take money from risk-averse savers and give them interest

❑ Banks invest the money in corporations $\Rightarrow$ Taking the country forward

❑ Venture capitalists take risks by investing in half-cooked ideas

❑ Startups take a risk by working in unchartered territories

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

Decisions with Risk

- Sell Insurance
- Buy Insurance
- Sell a stock
- Buy a stock
- Download a software application on your computer
- Update software

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

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

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/   ©2023 Raj Jain

Blockchain Generations

Utility
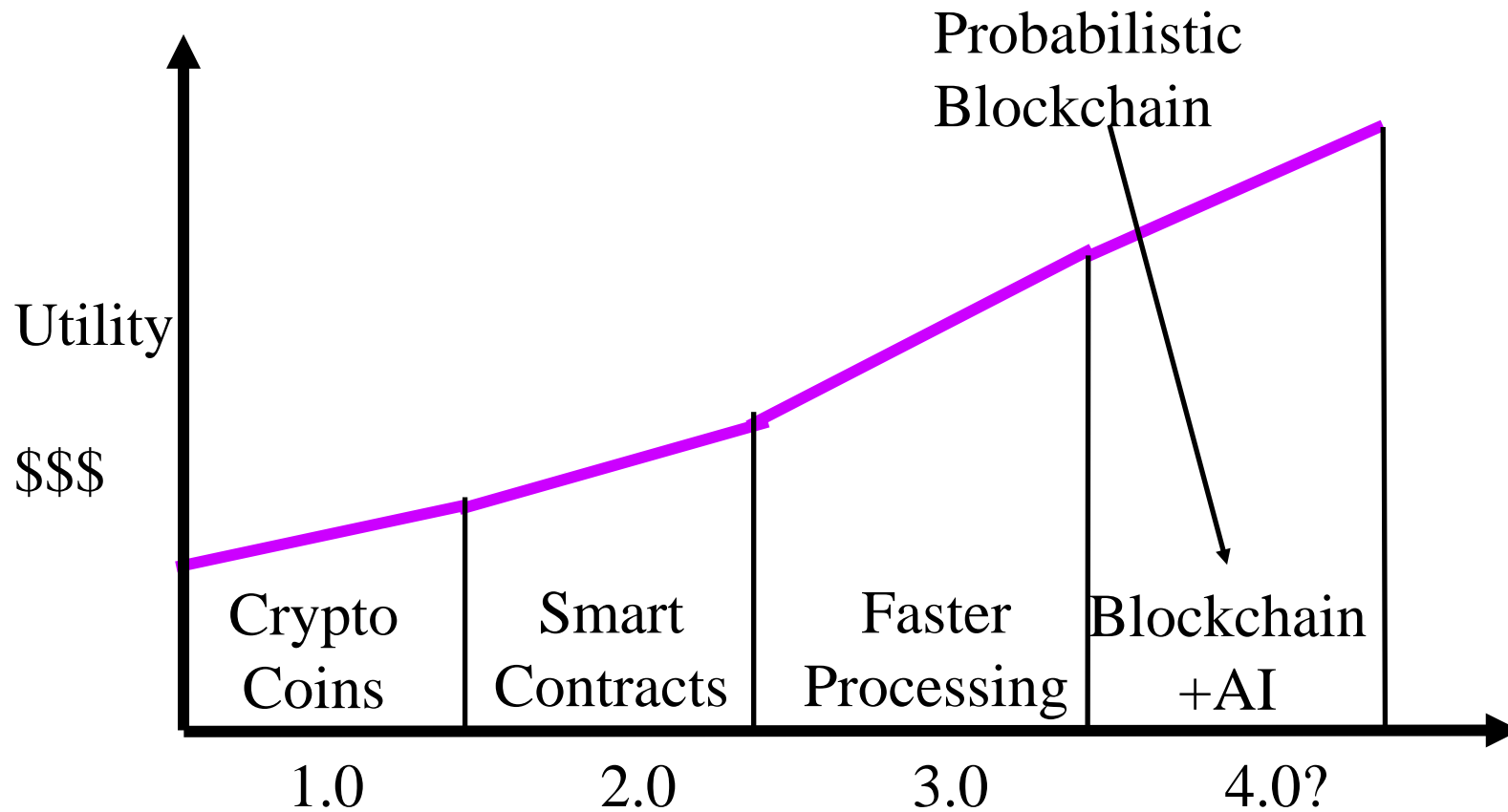
$$$

Probabilistic Blockchain

| Crypto Coins | Smart Contracts | Faster Processing | Blockchain +AI |

1.0   2.0   3.0   4.0?

http://www.cse.wustl.edu/~jain/cse570-23/

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.
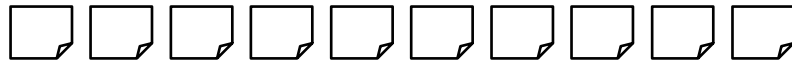
Limitation 3: Deterministic Events only

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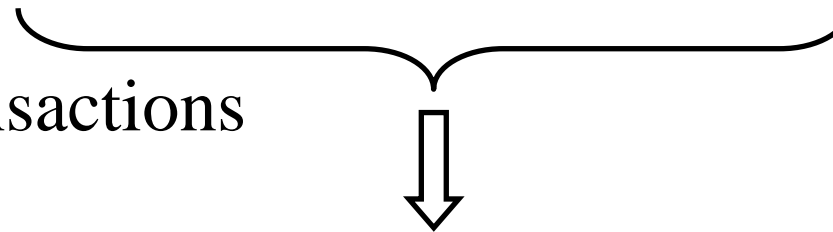

Student Questions

❑ Can you please explain limitation 2, line 2? *Only valid transactions are included. Non-valid transactions are discarded. There is no room for partially valid transactions.*

---

http://www.cse.wustl.edu/~jain/cse570-23/

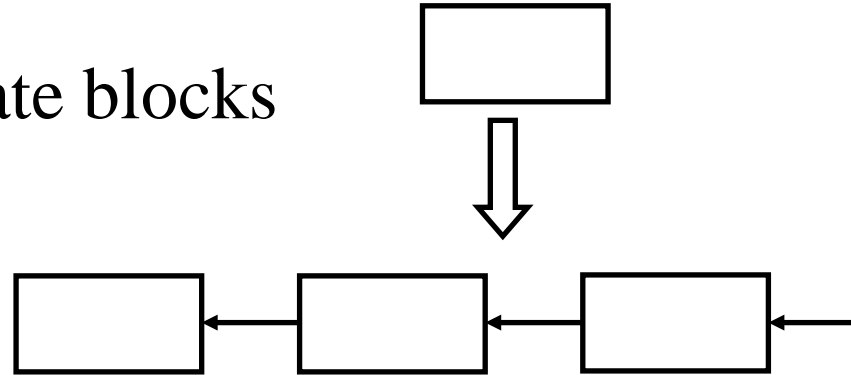©2023 Raj Jain

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

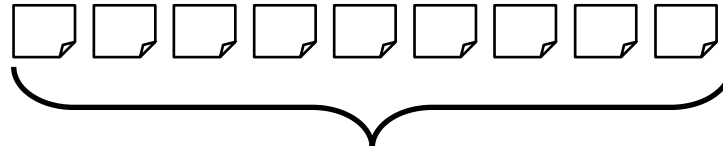- ❑ There are many users, many mining nodes and many blockchain nodes.

- ❑ More nodes ⇒ Better. Less ⇒ Blockchain not required/useful.

Student Questions

- ❑ Can a user also validate transactions and create blocks?

Yes, anyone can play any or all roles. But their blocks are likely to succeed if they have large computing power.

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

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 about the
  blockchain and use it for group decisions

http://www.cse.wustl.edu/~jain/cse570-23/

©2023 Raj Jain

17.44

Student Questions

❑ What are the benefits of being decentralized in your problem? Instead, for example, we can assume there is a logically centralized system that can infer knowledge from data.

Centralized systems exist. You need to trust the central authority.

❑ Blockchains can establish trust between nodes that do not necessarily trust each other by executing a consensus algorithm. What is your consensus algorithm, and why?

We do not specify any other parts of the blockchain. They work fine with all blockchains. You can use PoS, PoW, or whatever.

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 is the market going?

  ➢ Whether we should buy, sell, or hold?
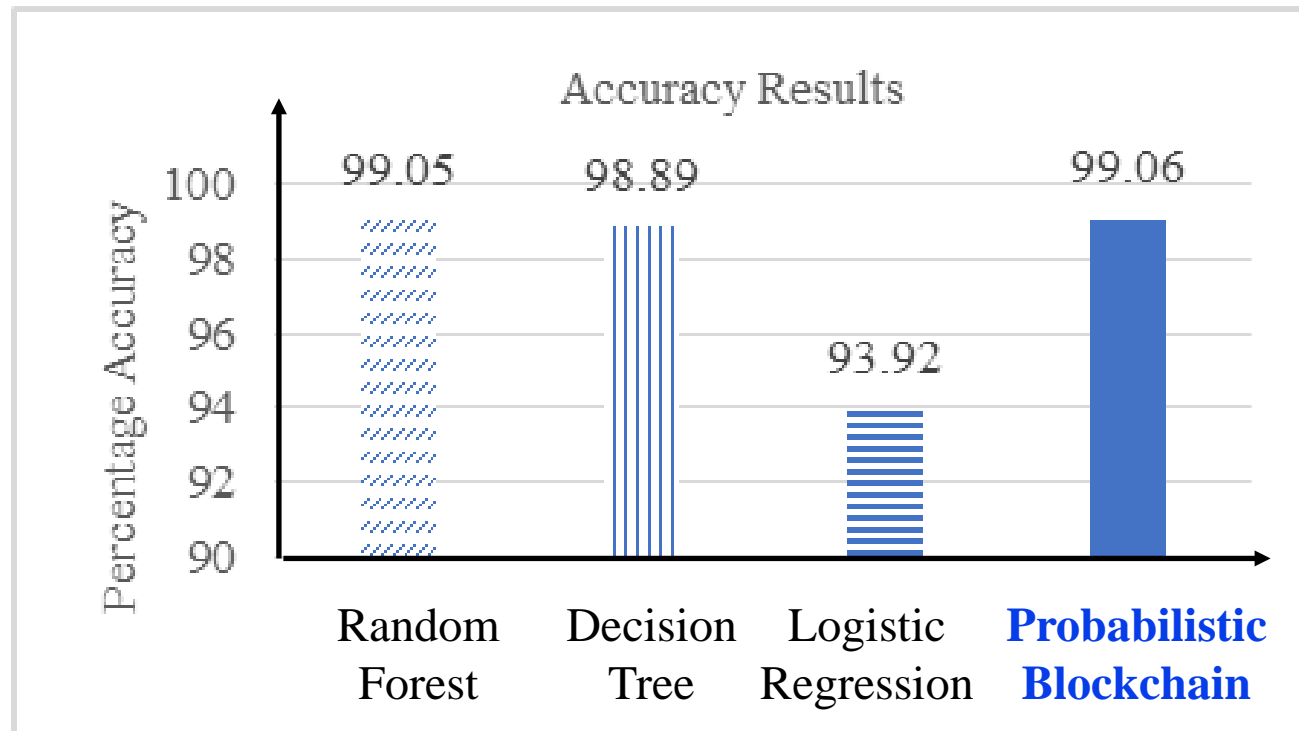
Student Questions

Empirical Validation

❑ Issue: Whether a network traffic pattern represents an intrusion

❑ 1000 Agents using different machine learning algorithms give their decisions: Yes or No

  ➢ Agents randomly pick one of the three algorithms:

    ❑ Random Forest, Decision Tree, Logistic Regression

❑ Mining nodes summarize these decisions using the majority function

Student Questions

❑ What do you mean by empirical validation?
Empirical=Based on observations

http://www.cse.wustl.edu/~jain/cse570-23/
©2023 Raj Jain

Results

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

Accuracy Results

99.05	98.89	93.92	99.06
Random Forest	Decision Tree	Logistic Regression	**Probabilistic Blockchain**

Percentage Accuracy: 90, 92, 94, 96, 98, 100

Distributed decision making is better than any individual decision

Summary
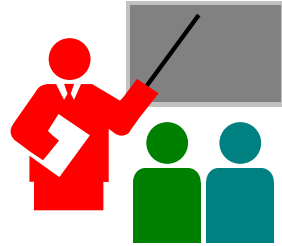
1. The current trend is to make everything decentralized

2. Bitcoin is a decentralized currency.

3. Blockchain 1.0 is used for global consensus on Bitcoin transactions.

4. Blockchain 3.0 allows sophisticated contracts, making it useful for many network and security applications

5. Probabilistic Blockchains allow probabilistic statements to make decisions under risk.

Reading List

❑ Koshik Raj, "Foundations of Blockchain," Packt Publishing, January 2019, ISBN: 9781789139396 (Safari Book)

❑ 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

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/

Other Readings

- A. M. Antonopoulos, "Mastering Bitcoin," Oreilly, 2014, 272 pp. (Safari Book)

- A. Lewis, "The Basics of Bitcoins and Blockchains," Mango Publishing, 2018, 408 pp.

- A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, "Bitcoin and Cryptocurrency Technology: A Comprehensive Introduction," Princeton University Press, 2016, 304 pp.

Student Questions

Online Resources

❑ CoinDesk: Bitcoin News, Prices, Charts, Guides & Analysis, http://www.coindesk.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

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/   ©2023 Raj Jain

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

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/
©2023 Raj Jain

Scan This to Download These Slides

Raj Jain

http://rajjain.com

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/m_17blc.htm

http://www.cse.wustl.edu/~jain/cse570-23/

17.53

Scan This to Download These Slides

Raj Jain

http://rajjain.com

Student Questions

http://www.cse.wustl.edu/~jain/cse570-23/m_17blc.htm

http://www.cse.wustl.edu/~jain/cse570-23/

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

Student Questions

Documentaries on Blockchains

- ❏ *Cryptopia: Bitcoin, and the future of the Internet, 1h 26 min, 2021
- ❏ *Banking on Africa – The Bitcoin Revolution, 47 min, 2020
- ❏ *Bit x Bit: In Bitcoin, we trust, 1h 17 min, 2019
- ❏ *The Blockchain and Us, 32 min 2017
- ❏ *Banking on Bitcoin, 2017
- ❏ Rizqi Presents: Blockchain Technology, 35 min, 2017
- ❏ Blockchain Technology,
- ❏ Blockchain City, 41 min, 2019
- ❏ How will Blockchain change the world, 8 min, 2020

*Amazon Prime Video: Free if you are a Prime member. This changes over time.

Student Questions