CPSC 422/522 Design & Implementation of Operating Systems

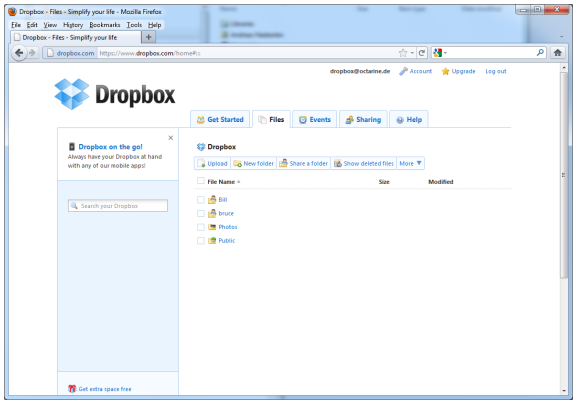
Lecture 22: Distributed Systems

Zhong Shao
Dept. of Computer Science
Yale University

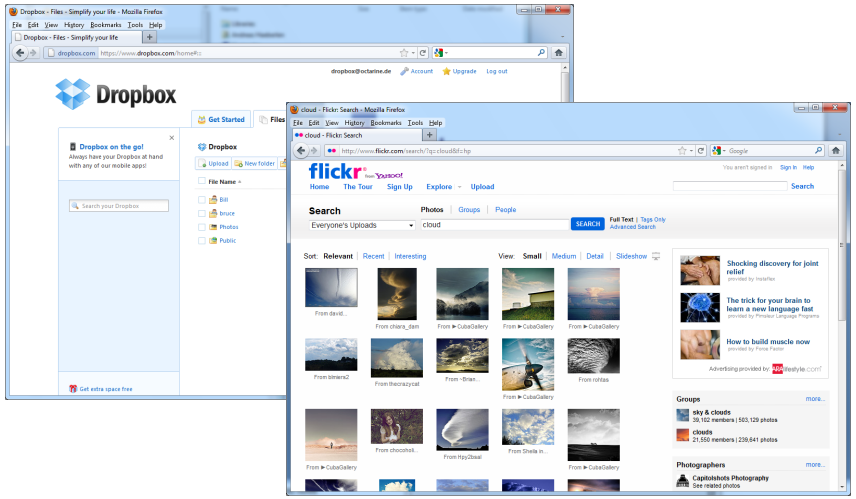
Acknowledgement: some slides are taken from previous lectures by Dr. Ennan Zhai

Have you used distributed system?

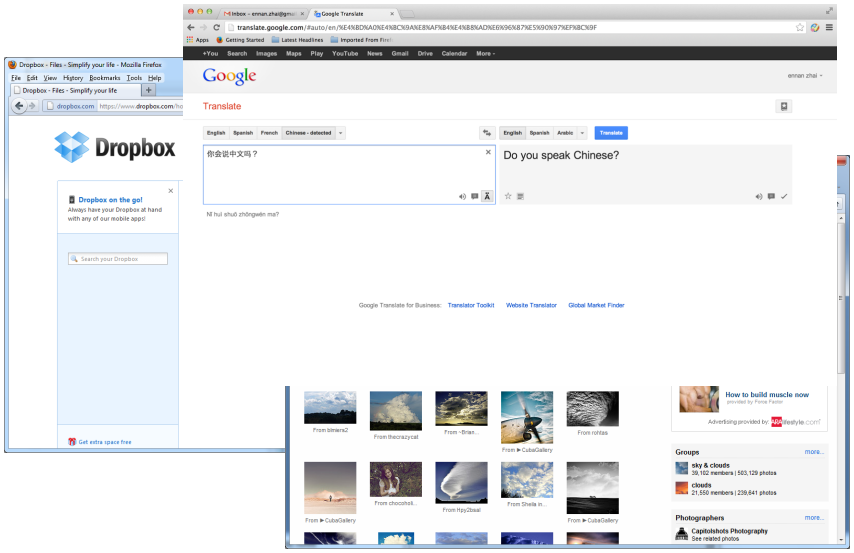
Have you used distributed system?



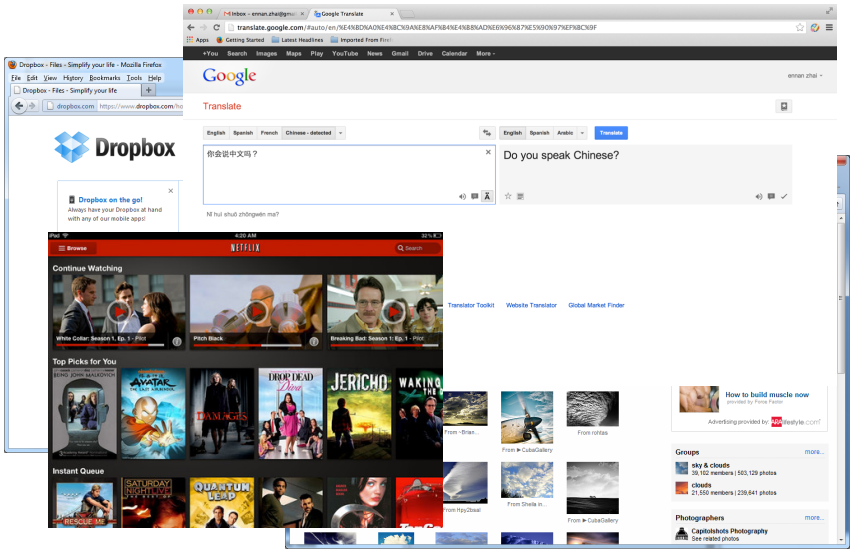
Have you used distributed system?



Have you used distributed system?



Have you used distributed system?



What is a distributed system?

- A system of multiple computers (nodes) communicating over a network

What is a distributed system?

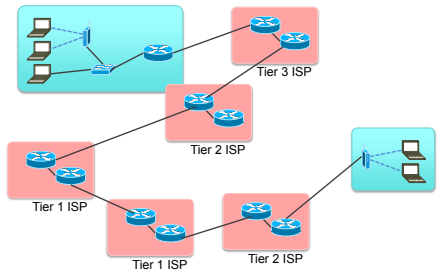
- A system of multiple computers (nodes) communicating over a network
- Some following questions:
  - What is a decentralized system?
  - What is a cloud system?
  - What is a centralized distributed system?

Network Basics

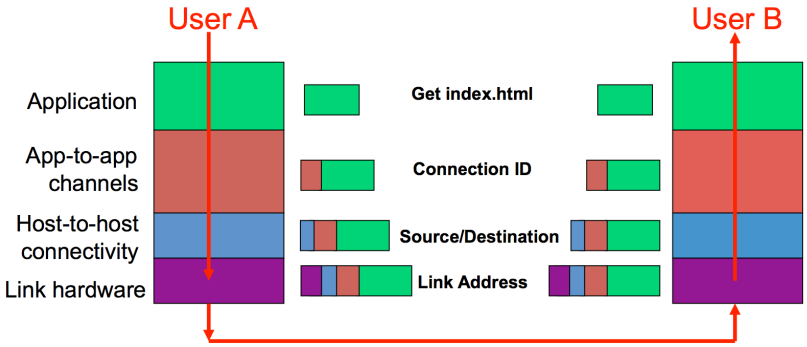
- We connect computers via point-to-point links:
  - Local area network, DNS and ISP routers
  - Communications are unreliable
  - No global control of the network

Network Basics

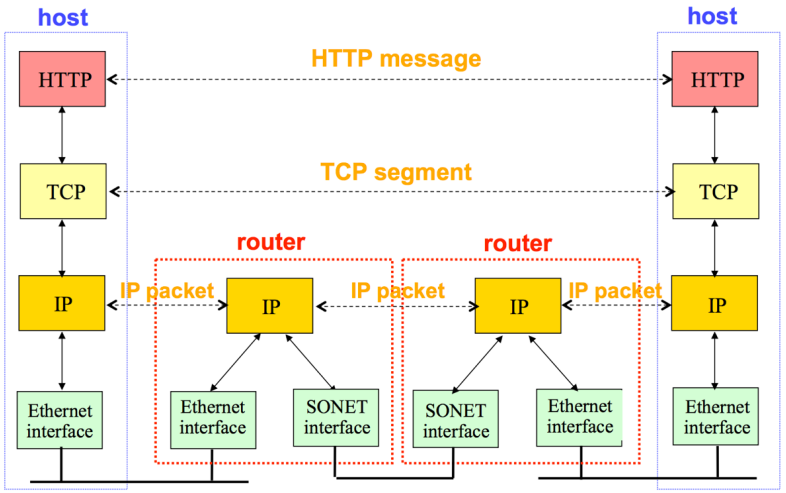
- We connect computers via point-to-point links:
  - Local area network, DNS and ISP routers
  - Communications are unreliable
  - No global control of the network



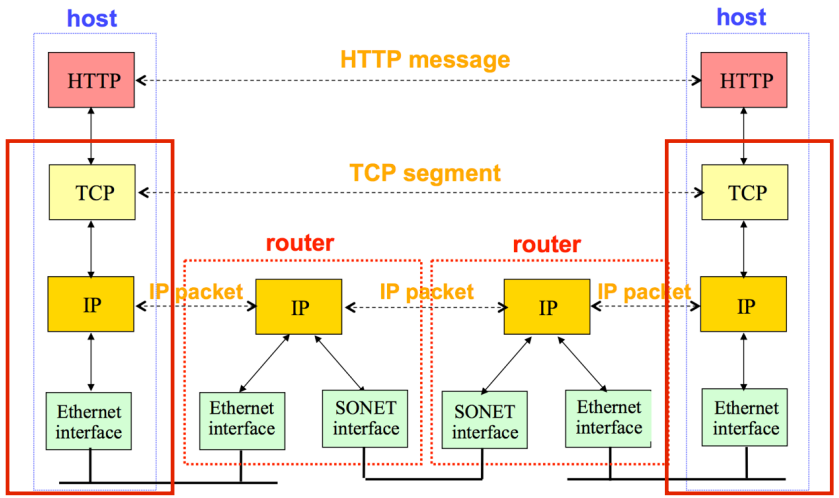
Example: HTTP Layer Encapsulation



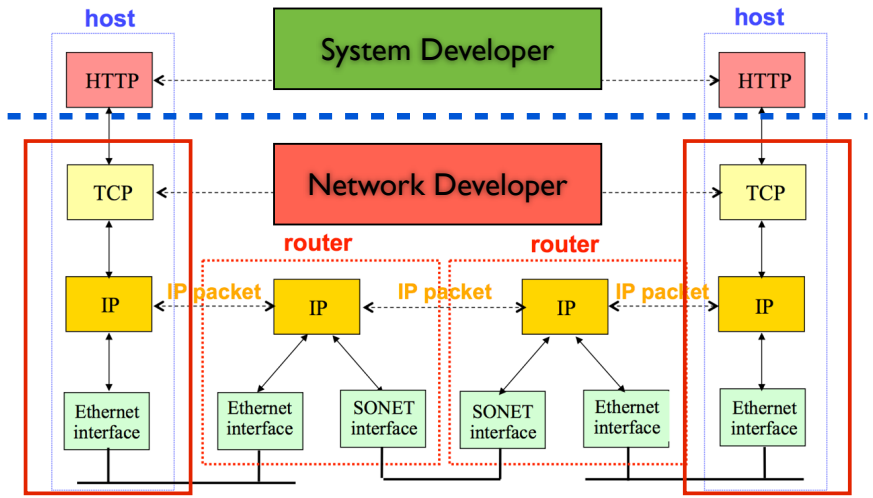
End Hosts vs. Routers



End Hosts vs. Routers



End Hosts vs. Routers



Finding Nodes

Network Basics

- Each interface on a host has a unique MAC address:
  - My machine 48-bit ethernet address = 32:00:19:ac:b1:40

Network Basics

- Each interface on a host has a unique MAC address:
  - My machine 48-bit ethernet address = 32:00:19:ac:b1:40

Why we need a physical address?

Network Basics

- Each interface on a host has a unique MAC address:
  - My machine 48-bit ethernet address = 32:00:19:ac:b1:40

Why we need a physical address?

Which layer in OSI model it belongs to?

Network Basics

- Each interface on a host has a unique MAC address:
  - My machine 48-bit ethernet address = 32:00:19:ac:b1:40

- This is *not* too interesting to us as programmers
  - We usually do not communicate at the data link layer

Network Basics

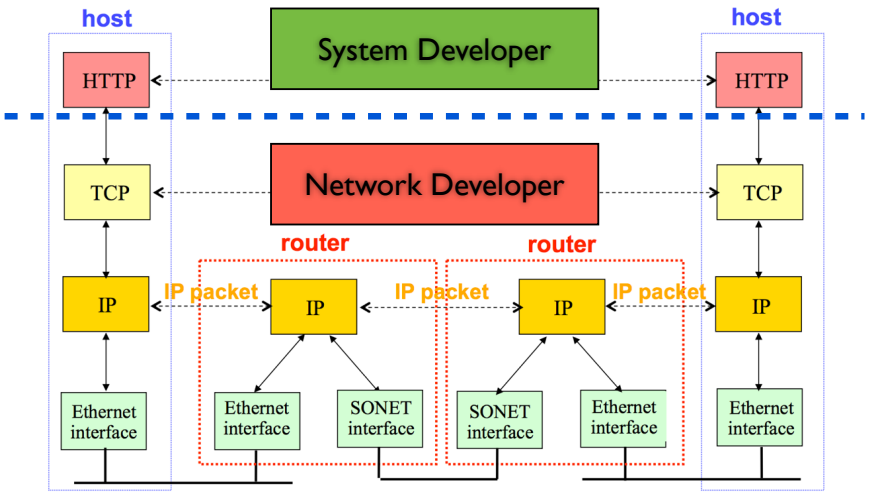
- Addressing applications:
  - IP address (32-bit for IPv4) and port number (16-bit)
  - Well-known port numbers (0-1023), e.g., ftp, ssh and http

Network Basics

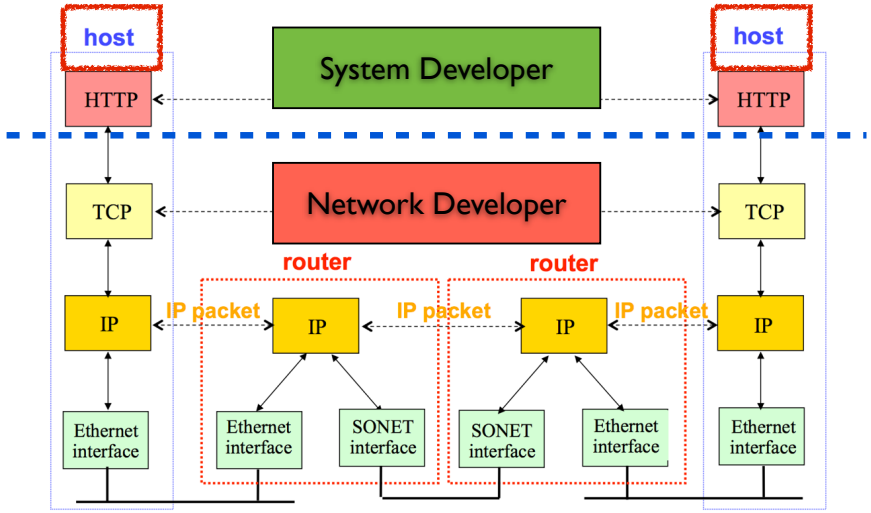
- Addressing applications:
  - IP address (32-bit for IPv4) and port number (16-bit)
  - Well-known port numbers (0-1023), e.g., ftp, ssh and http

- We have two transport-layer protocols
  - TCP (SSH and FTP) and UDP (Streaming and local broadcast)
  - What is the difference?

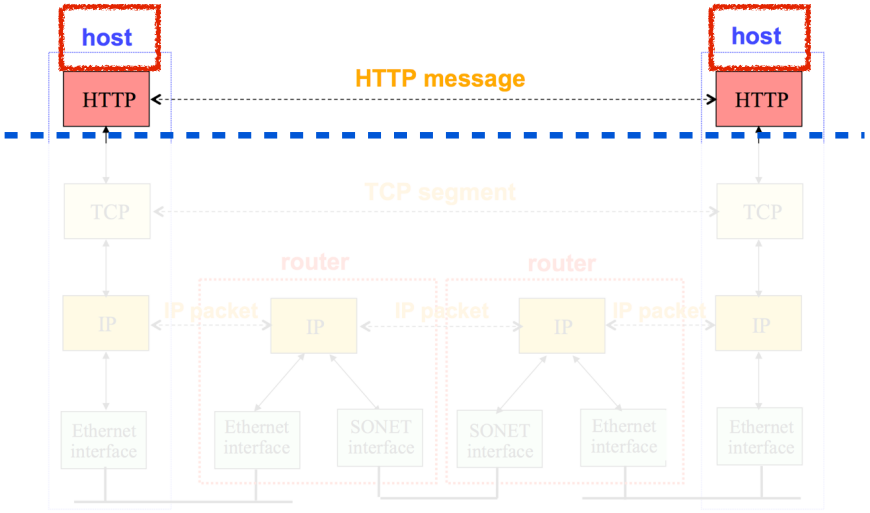
End Hosts vs. Routers



End Hosts vs. Routers



End Hosts vs. Routers



Today's Cluster

PC

Today's Cluster

PC

Server

Today's Cluster

PC

Server

Cluster

Today's Cluster

Today's Cluster

Rack

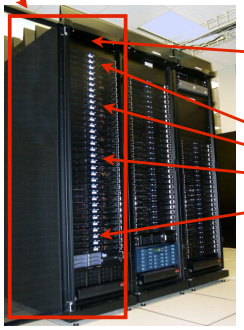
Today's Cluster

Rack

Network switches (connects nodes with each other and with other racks)

Today's Cluster

Rack

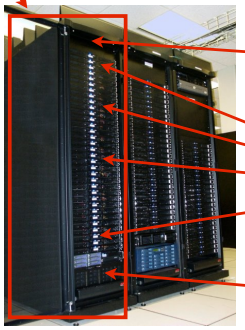


Network switches (connects nodes with each other and with other racks)

Many nodes/blades (often identical)

Today's Cluster

Rack



Network switches (connects nodes with each other and with other racks)

Many nodes/blades (often identical)

Storage device(s)

Today's Cluster


PC


Server


Cluster

- What if cluster is too big to fit into machine room?

Datacenter


PC


Server


Cluster

- What if cluster is too big to fit into machine room?
  - Build a separate building for the cluster
  - Building can have lots of cooling and power

Datacenter


PC


Server


Cluster


Data center

- What if cluster is too big to fit into machine room?
  - Build a separate building for the cluster
  - Building can have lots of cooling and power
  - Result: Data center

Google Datacenter in Oregon

Google Datacenter in Oregon

Data centers (size of a football field)

Google Datacenter in Oregon

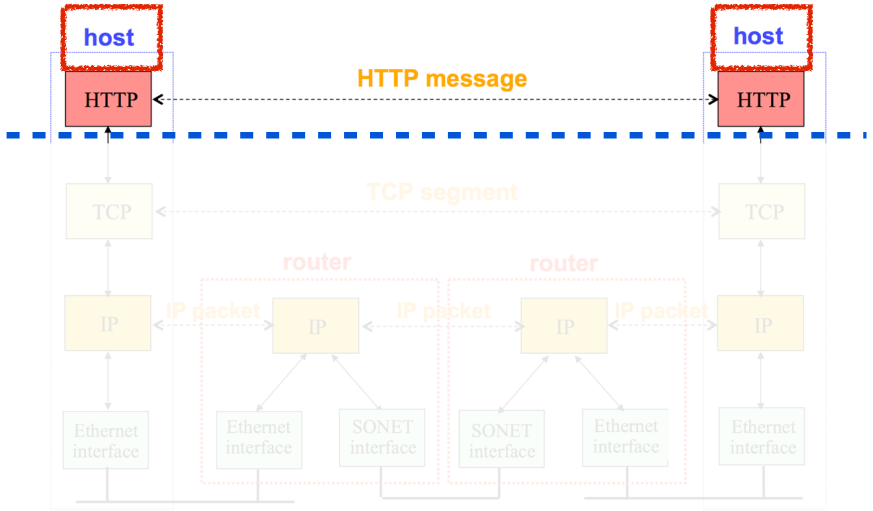
Data centers (size of a football field)

- A warehouse-sized computer
  - A single data center can easily contain 10,000 racks with 100 cores in each rack (1,000,000 cores total)

Google Datacenters in the US

Google Datacenters in this World

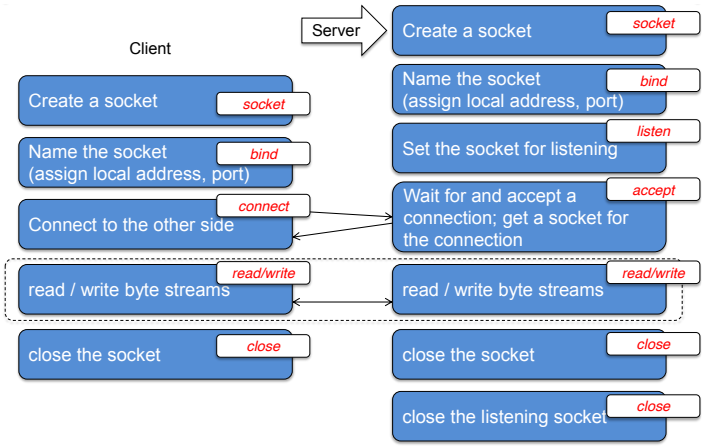
End Hosts vs. Routers



Network APIs

- Programmers need to access the network
- A network application programming interface (API)
  - Socket programming
  - Remote procedure calls

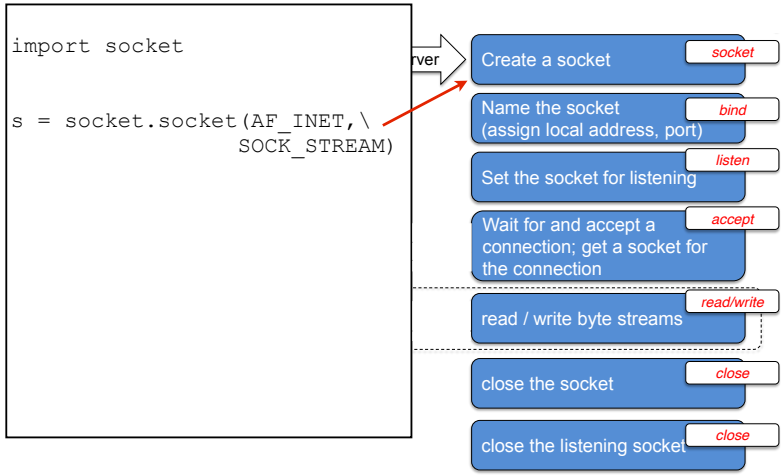
Socket (TCP)



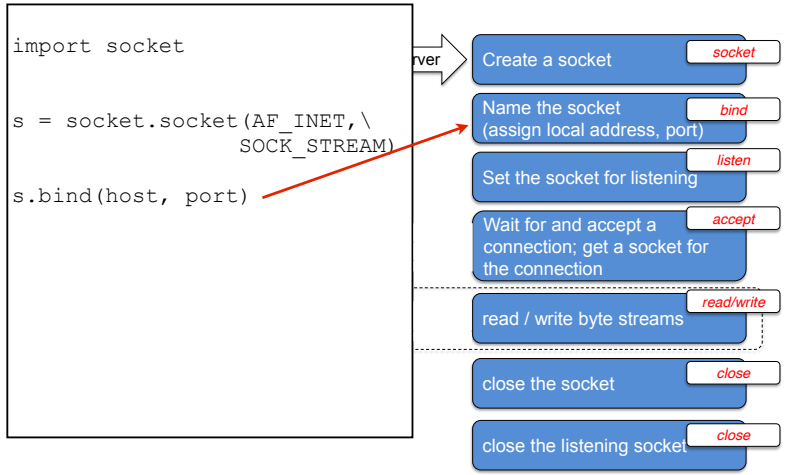
Socket (TCP)

```
import socket
```

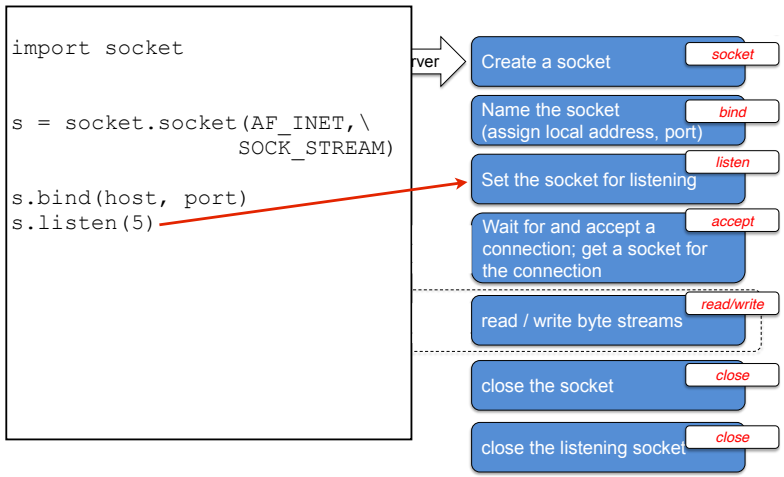
Socket (TCP)



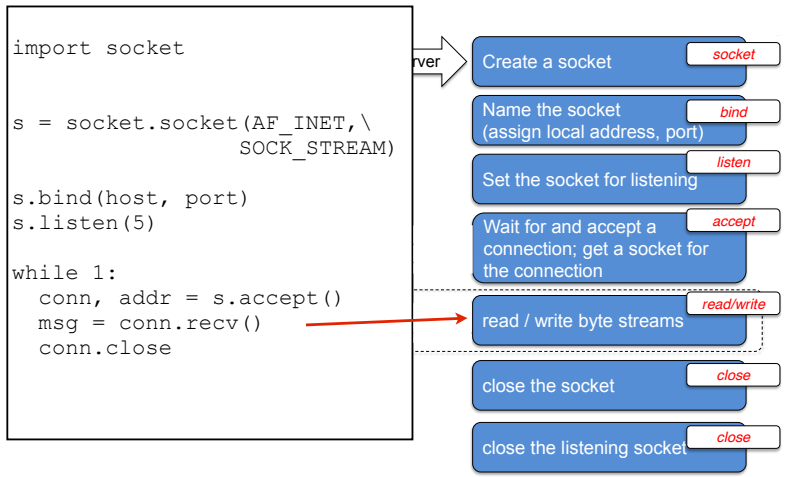
Socket (TCP)



Socket (TCP)



Socket (TCP)



Socket (TCP)

```
import socket


s = socket.socket(AF_INET,\
                  SOCK_STREAM)

s.bind(host, port)
s.listen(5)

while 1:
  conn, addr = s.accept()
  msg = conn.recv()
  conn.close

s.close
```

rver

- Create a socket — *socket*
- Name the socket (assign local address, port) — *bind*
- Set the socket for listening — *listen*
- Wait for and accept a connection; get a socket for the connection — *accept*
- read / write byte streams — *read/write*
- close the socket — *close*
- close the listening socket — *close*

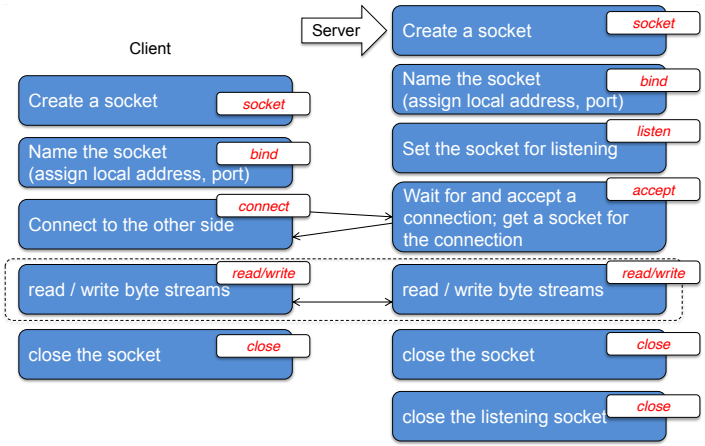
Socket (TCP)

Client

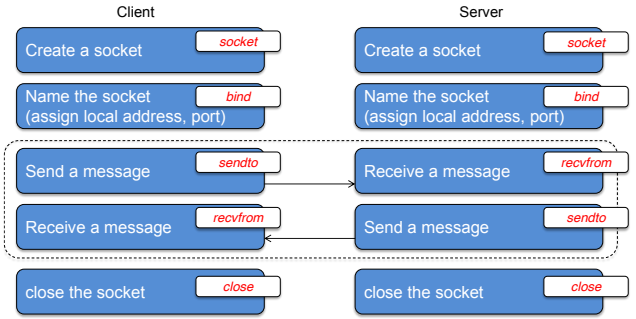
- Create a socket — *socket*
- Name the socket (assign local address, port) — *bind*
- Connect to the other side — *connect*
- read / write byte streams — *read/write*
- close the socket — *close*

```
import socket


s = socket.socket(AF_INET,\
                  SOCK_STREAM)

a = socket.gethostbyname(host)
s.connect(a, port)
s.sendall(msg)
```

Socket (TCP)



Socket (UDP)



What's the Cloud Computing

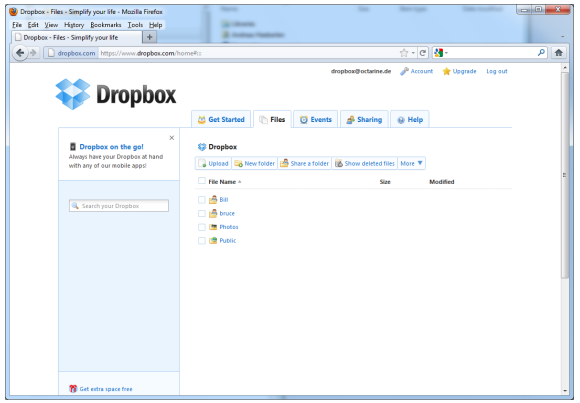
What's the Cloud Computing

Cloud computing is a business model for enabling convenient network access to a shared pool of configurable resources which can be rapidly provisioned and released with minimal management effort or service provider interaction.

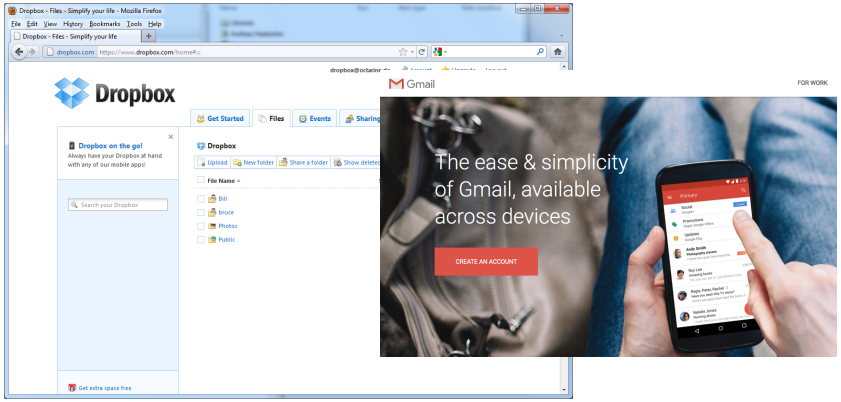
--- according to NIST(National Institute of Standards and Technology)

Have You Used the Cloud?

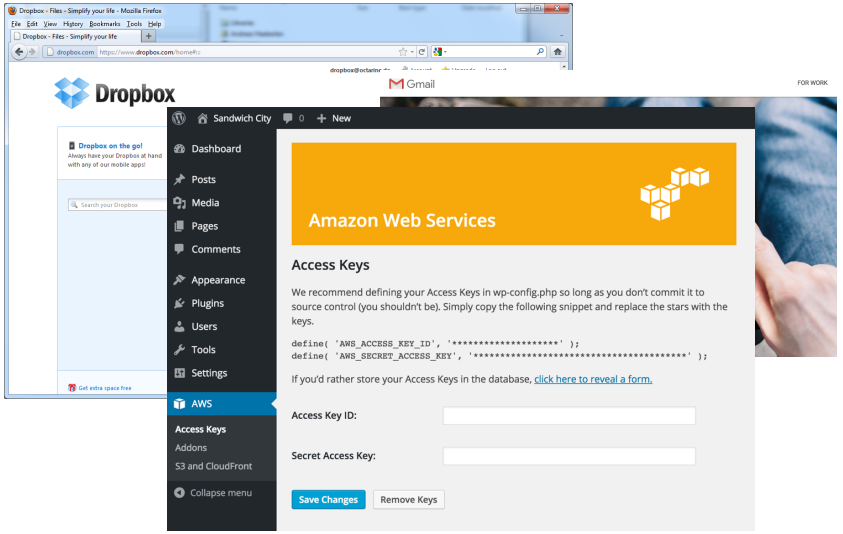
Have You Used the Cloud?



Have You Used the Cloud?



Have You Used the Cloud?



Why We Like It?

Why We Like It?

- Why users like it?
  - Do not care where it is, it is "just there"
  - Access from "any" platform

Why We Like It?

- Why users like it?
  - Do not care where it is, it is "just there"
  - Access from "any" platform

Cloud Services v.s. Traditional Distributed Systems

Why We Like It?

- Why users like it?
  - Do not care where it is, it is "just there"
  - Access from "any" platform
- Why CS researchers like it?
  - High-performance computation with less money
  - Lots of *hard* and *interesting* new challenges

Building Blocks

- What techniques are used to support cloud?
  - Internet
  - Smart and cheap personal devices
  - Robust and scalable software systems
  - Virtualization
  - ... ...

Types of Cloud Services

- Three types of services:

Types of Cloud Services

- Three types of services:

  it.

  - Infrastructure as a Service (IaaS)
    - Analogy: Grocery store. Provides raw ingredients.

Types of Cloud Services

- Three types of services:

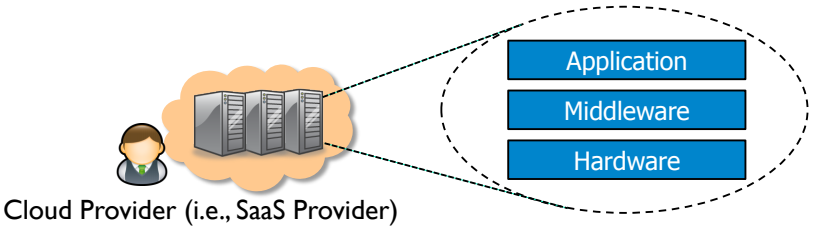
  - Platform as a Service (PaaS)
    - Analogy: Take-out food. Prepares meal but does not serve it.
  - Infrastructure as a Service (IaaS)
    - Analogy: Grocery store. Provides raw ingredients.

Types of Cloud Services

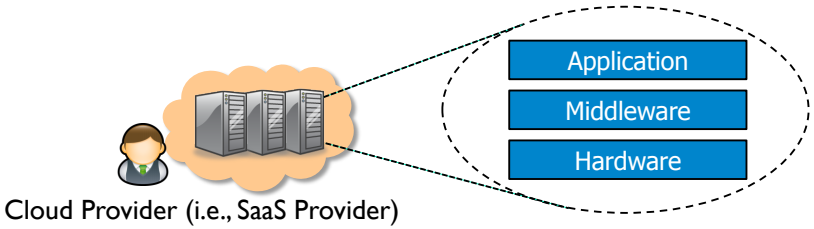
- Three types of services:
  - Software as a Service (SaaS)
    - Analogy: Restaurant. Prepares&serves entire meal, does the dishes, etc
  - Platform as a Service (PaaS)
    - Analogy: Take-out food. Prepares meal but does not serve it.
  - Infrastructure as a Service (IaaS)
    - Analogy: Grocery store. Provides raw ingredients.

Software as a Service (SaaS)

Software as a Service (SaaS)

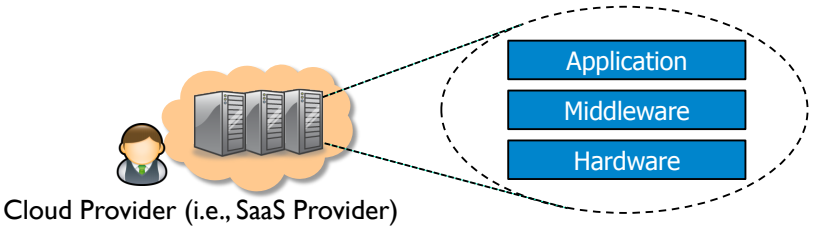


Software as a Service (SaaS)



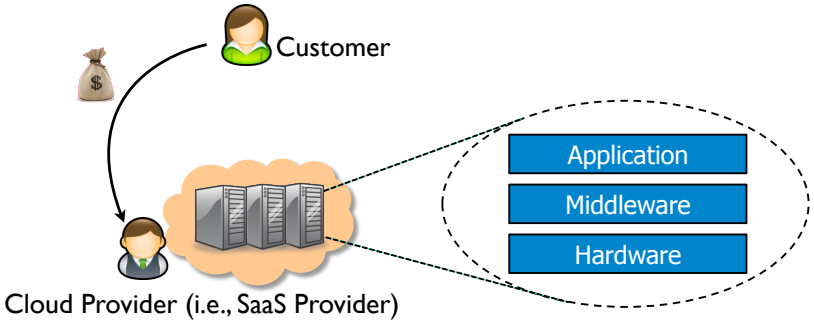
- SaaS provider offers an entire application

Software as a Service (SaaS)



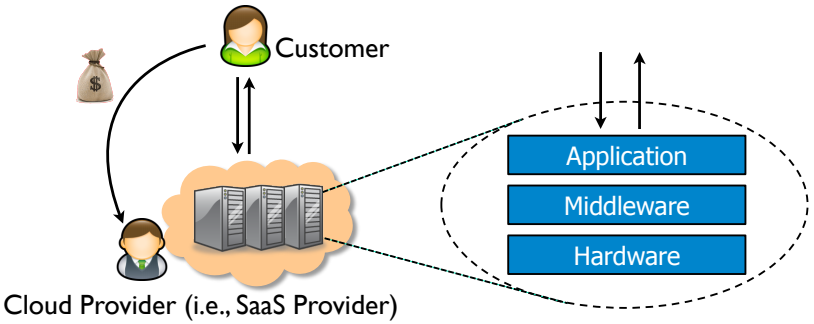
- SaaS provider offers an entire application
  - Word processor, spreadsheet, CRM software, etc.

Software as a Service (SaaS)



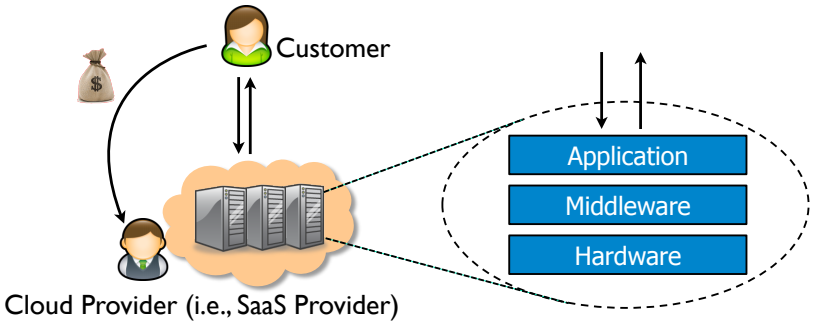
- SaaS provider offers an entire application
  - Word processor, spreadsheet, CRM software, etc.
  - Customer pays cloud provider and uses the service

Software as a Service (SaaS)



- SaaS provider offers an entire application
  - Word processor, spreadsheet, CRM software, etc.
  - Customer pays cloud provider and uses the service

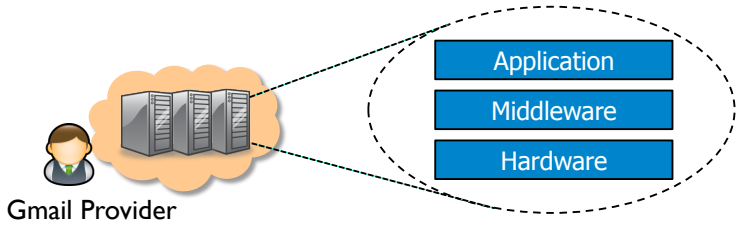
Software as a Service (SaaS)



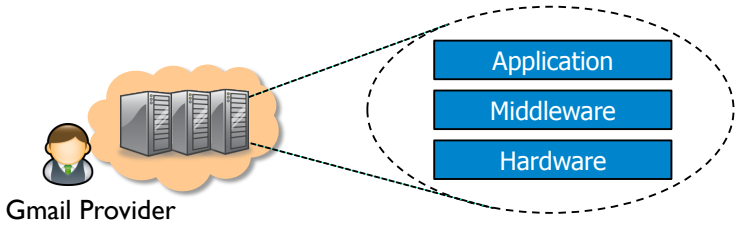
- SaaS provider offers an entire application
  - Word processor, spreadsheet, CRM software, etc.
  - Customer pays cloud provider and uses the service
  - Example: Google Apps, Salesforce.com, etc.

SaaS Example: Gmail

SaaS Example: Gmail

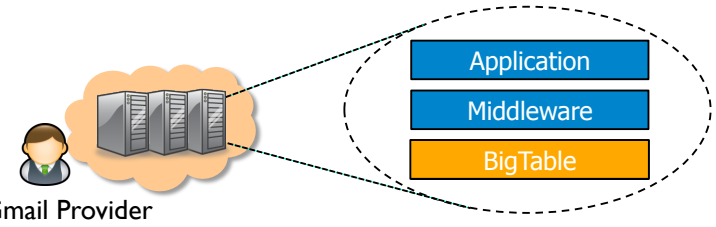


SaaS Example: Gmail



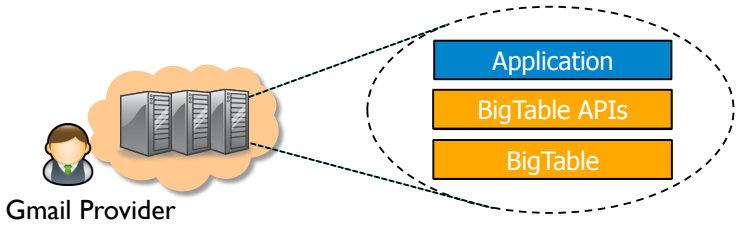
- Outsourcing your e-mail software:
  - Distributed, replicated message store in BigTable

SaaS Example: Gmail



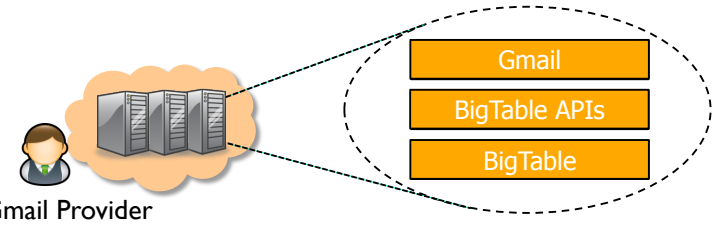
- Outsourcing your e-mail software:
  - Distributed, replicated message store in BigTable

SaaS Example: Gmail



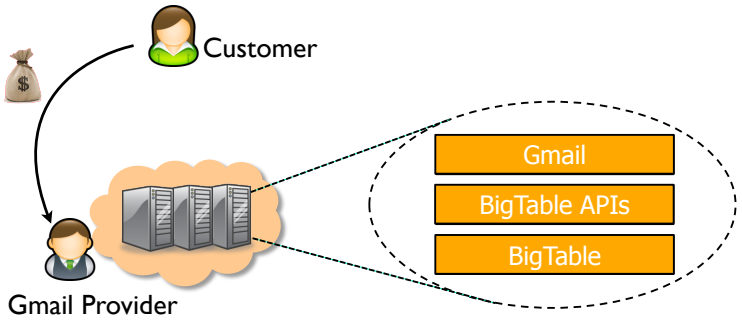
- Outsourcing your e-mail software:
  - Distributed, replicated message store in BigTable

SaaS Example: Gmail



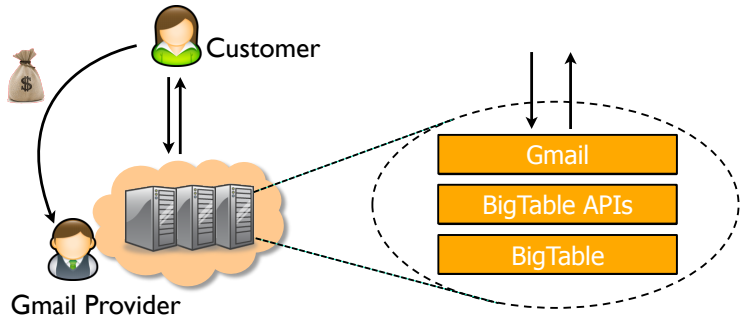
- Outsourcing your e-mail software:
  - Distributed, replicated message store in BigTable

SaaS Example: Gmail



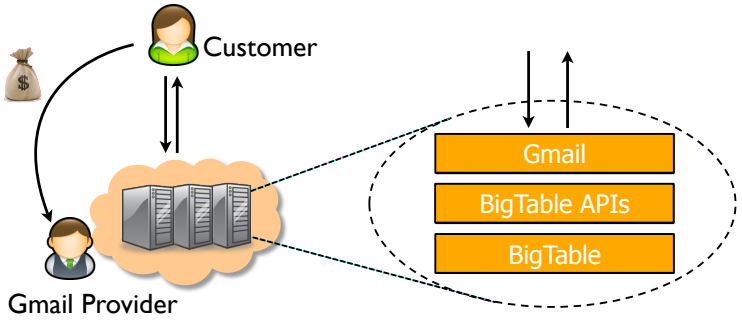
- Outsourcing your e-mail software:
  - Distributed, replicated message store in BigTable

SaaS Example: Gmail



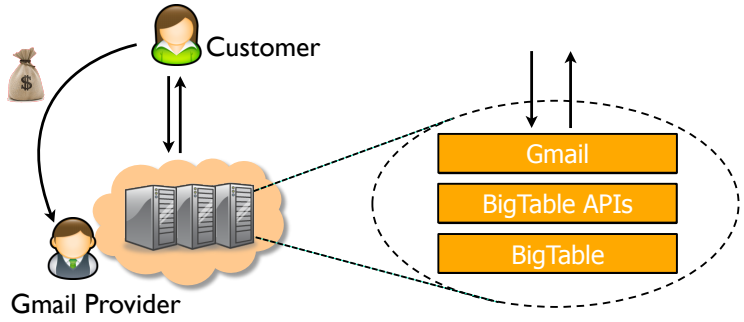
- Outsourcing your e-mail software:
  - Distributed, replicated message store in BigTable

SaaS Example: Gmail



- Outsourcing your e-mail software:
  - Distributed, replicated message store in BigTable
  - Weak consistency model for some operations (e.g., msg read)

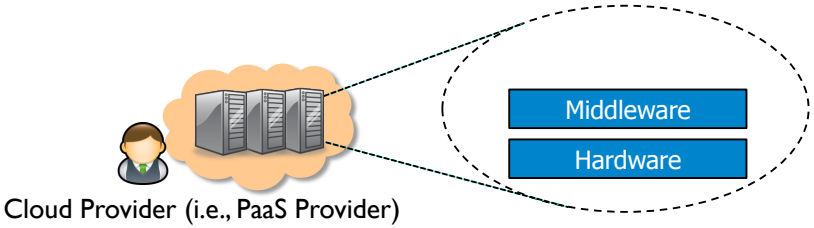
SaaS Example: Gmail



- Outsourcing your e-mail software:
  - Distributed, replicated message store in BigTable
  - Weak consistency model for some operations (e.g., msg read)
  - Stronger consistency for others (e.g., send msg)

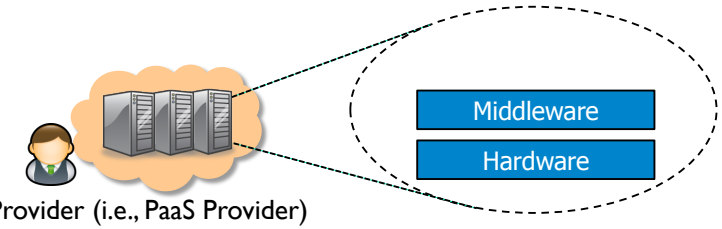
Platform as a Service (PaaS)

Platform as a Service (PaaS)



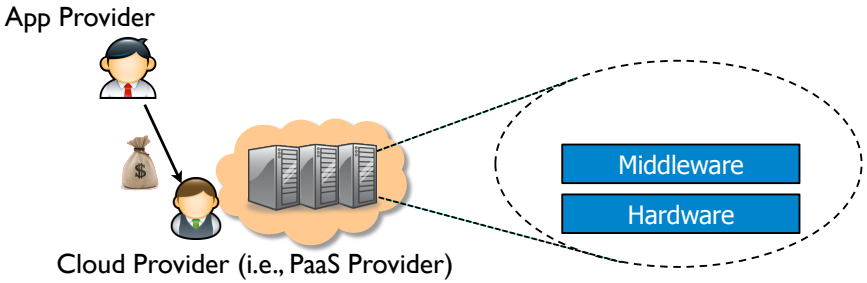
- Cloud provides middleware/infrastructure

Platform as a Service (PaaS)



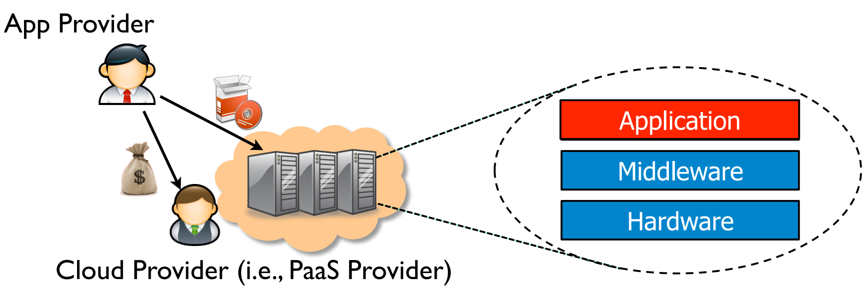
- Cloud provides middleware/infrastructure
  - For example, Microsoft Common Language Runtime (CLR)

Platform as a Service (PaaS)



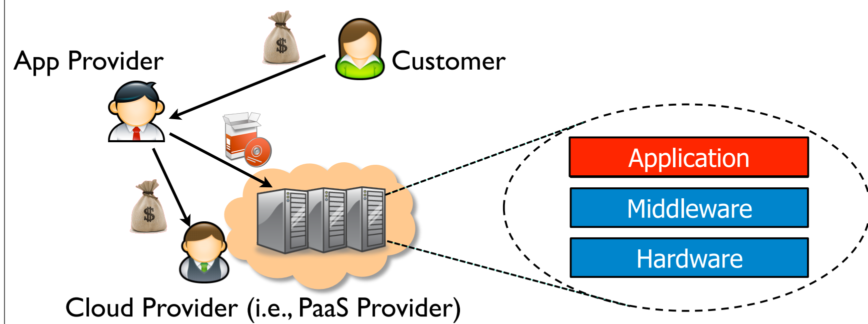
- Cloud provides middleware/infrastructure
  - For example, Microsoft Common Language Runtime (CLR)
  - App provider pays the cloud for the platform

Platform as a Service (PaaS)



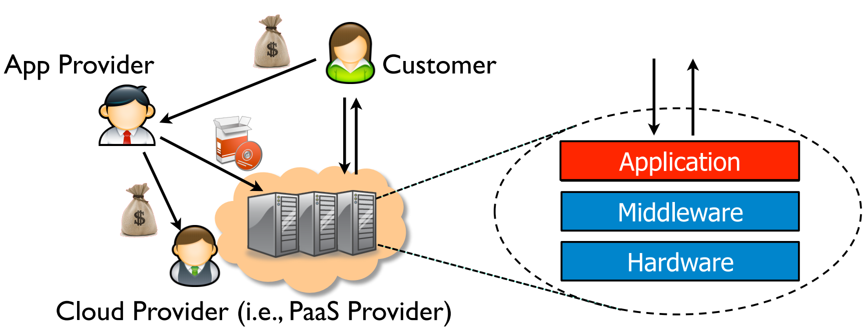
- Cloud provides middleware/infrastructure
  - For example, Microsoft Common Language Runtime (CLR)
  - App provider pays the cloud for the platform

Platform as a Service (PaaS)



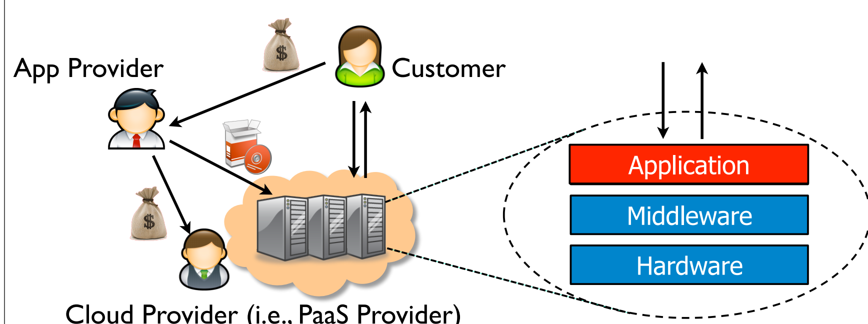
- Cloud provides middleware/infrastructure
  - For example, Microsoft Common Language Runtime (CLR)
  - App provider pays the cloud for the platform
  - Customer pays app provider for the service

Platform as a Service (PaaS)



- Cloud provides middleware/infrastructure
  - For example, Microsoft Common Language Runtime (CLR)
  - App provider pays the cloud for the platform
  - Customer pays app provider for the service

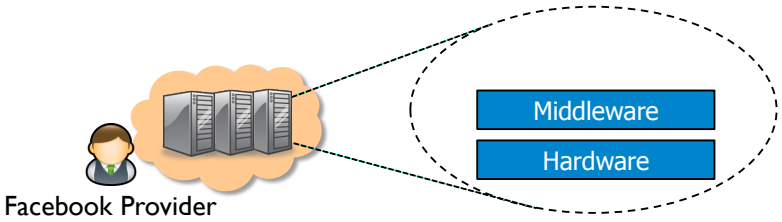
Platform as a Service (PaaS)



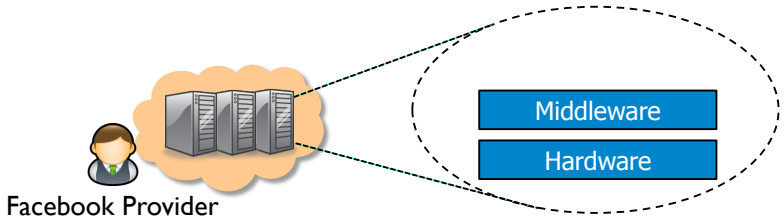
- Cloud provides middleware/infrastructure
  - For example, Microsoft Common Language Runtime (CLR)
  - App provider pays the cloud for the platform
  - Customer pays app provider for the service
  - Example: Windows Azure, Google App Engine, etc.

PaaS Example: Facebook

PaaS Example: Facebook

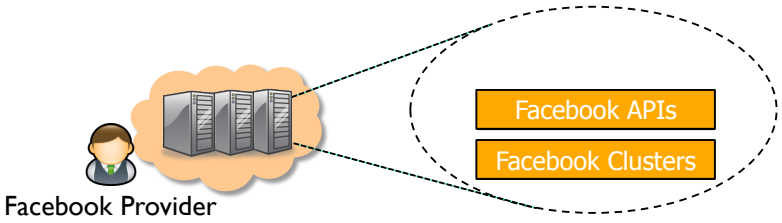


PaaS Example: Facebook



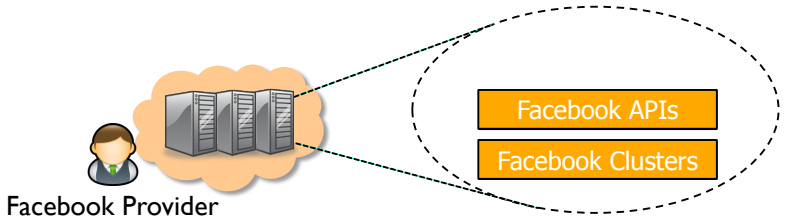
- Facebook offers PaaS capabilities to App provider

PaaS Example: Facebook



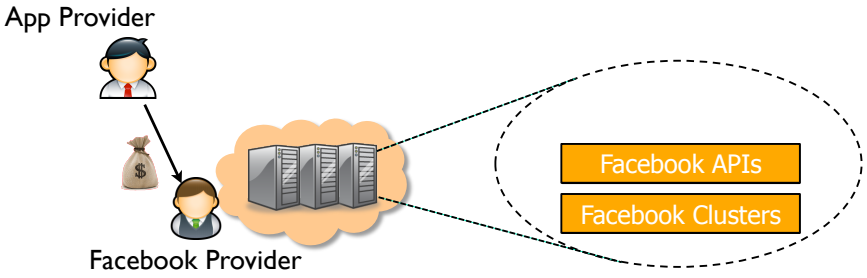
- Facebook offers PaaS capabilities to App provider

PaaS Example: Facebook



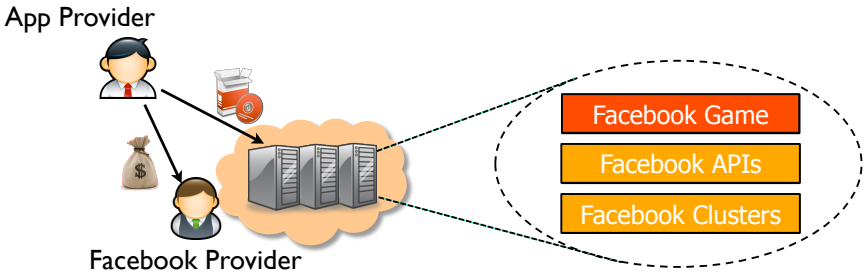
- Facebook offers PaaS capabilities to App provider
  - Facebook APIs allow access to social network properties

PaaS Example: Facebook



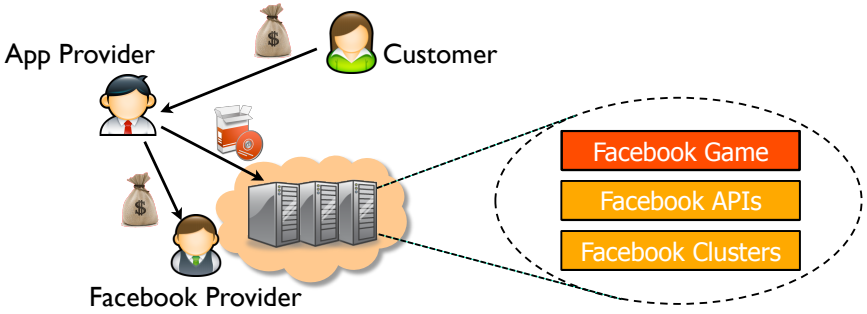
- Facebook offers PaaS capabilities to App provider
  - Facebook APIs allow access to social network properties
  - App providers adopt their services (e.g., game) onto Facebook

PaaS Example: Facebook



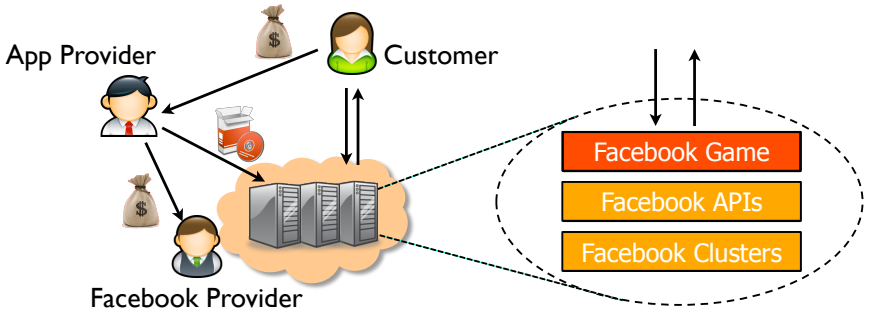
- Facebook offers PaaS capabilities to App provider
  - Facebook APIs allow access to social network properties
  - App providers adopt their services (e.g., game) onto Facebook

PaaS Example: Facebook



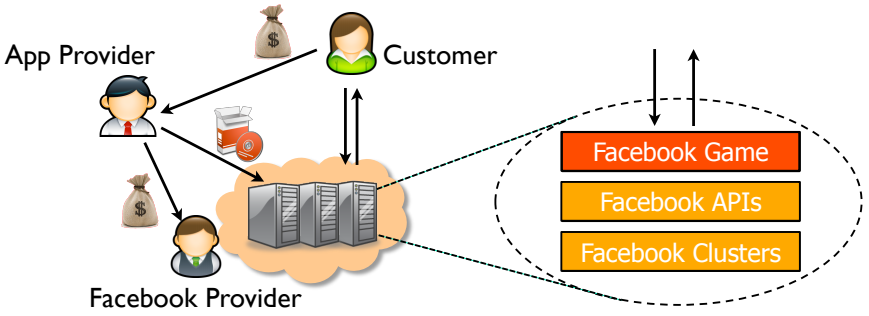
- Facebook offers PaaS capabilities to App provider
  - Facebook APIs allow access to social network properties
  - App providers adopt their services (e.g., game) onto Facebook

PaaS Example: Facebook



- Facebook offers PaaS capabilities to App provider
  - Facebook APIs allow access to social network properties
  - App providers adopt their services (e.g., game) onto Facebook

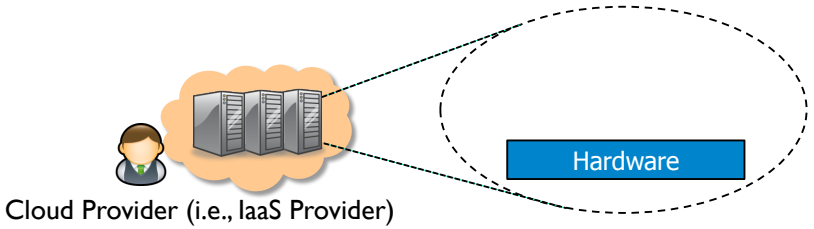
PaaS Example: Facebook



- Facebook offers PaaS capabilities to App provider
  - Facebook APIs allow access to social network properties
  - App providers adopt their services (e.g., game) onto Facebook
  - Facebook itself also uses PaaS provided by its company, e.g., log analysis for recommendations

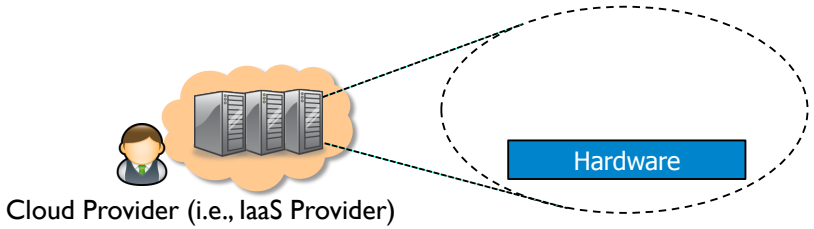
Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS)



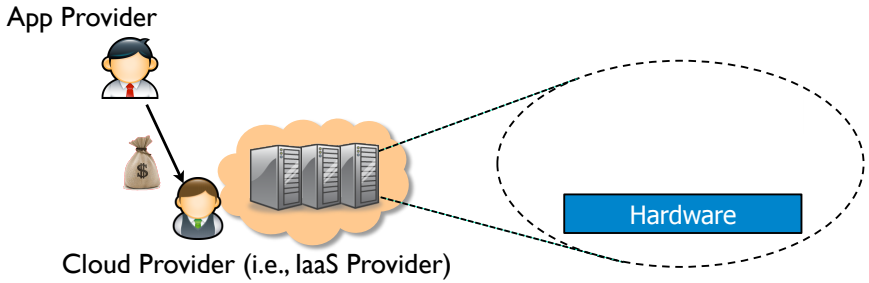
- Cloud provides raw computing resources

Infrastructure as a Service (IaaS)



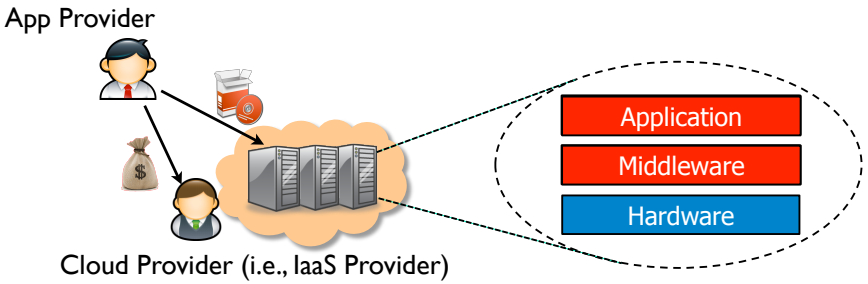
- Cloud provides raw computing resources
  - Virtual machines, blade servers, hard disk, etc.

Infrastructure as a Service (IaaS)



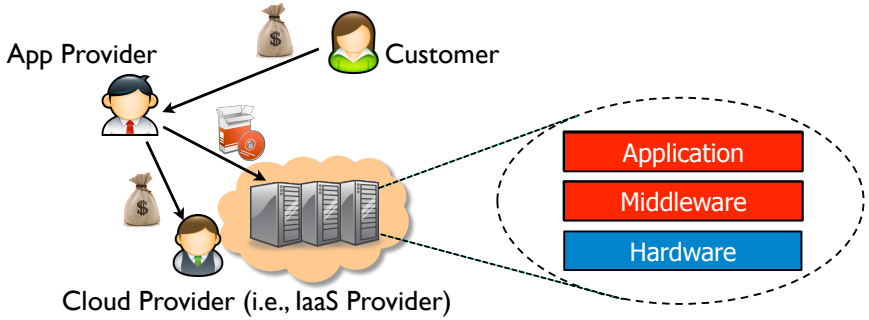
- Cloud provides raw computing resources
  - Virtual machines, blade servers, hard disk, etc.
  - App provider pays the cloud for the resources

Infrastructure as a Service (IaaS)



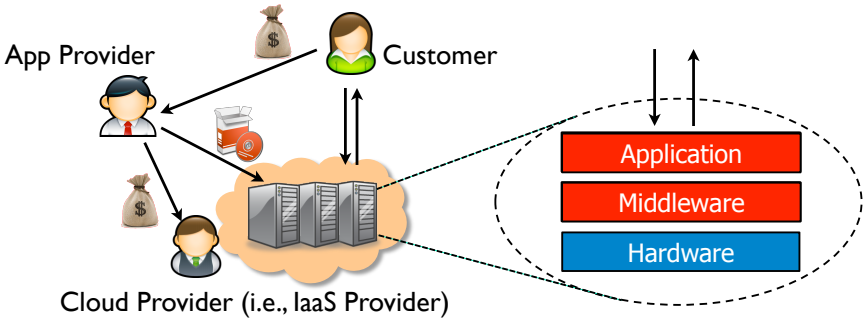
- Cloud provides raw computing resources
  - Virtual machines, blade servers, hard disk, etc.
  - App provider pays the cloud for the resources

Infrastructure as a Service (IaaS)



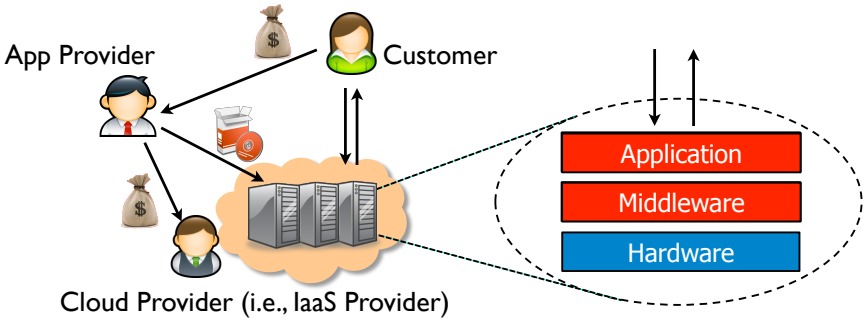
- Cloud provides raw computing resources
  - Virtual machines, blade servers, hard disk, etc.
  - App provider pays the cloud for the resources
  - Customer pays App provider for the service

Infrastructure as a Service (IaaS)



- Cloud provides raw computing resources
  - Virtual machines, blade servers, hard disk, etc.
  - App provider pays the cloud for the resources
  - Customer pays App provider for the service

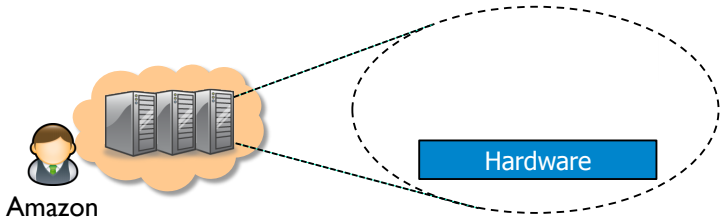
Infrastructure as a Service (IaaS)



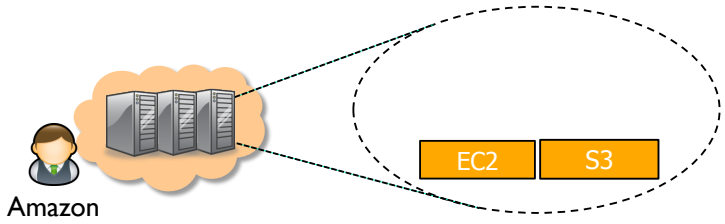
- Cloud provides raw computing resources
  - Virtual machines, blade servers, hard disk, etc.
  - App provider pays the cloud for the resources
  - Customer pays App provider for the service
  - Example: Amazon Web Services, Rackspace Cloud, etc.

IaaS Example: EC2 and S3

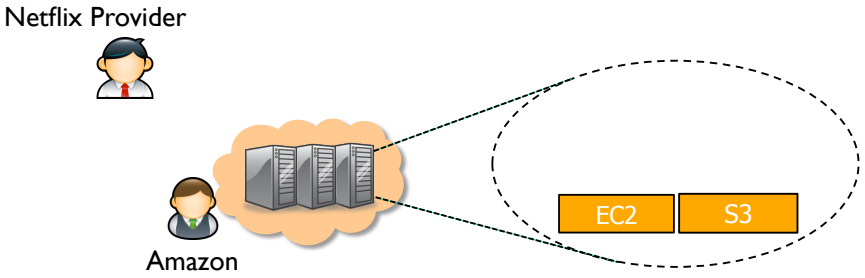
(Elastic Compute Cloud & Simple Storage Service)



IaaS Example: EC2 and S3

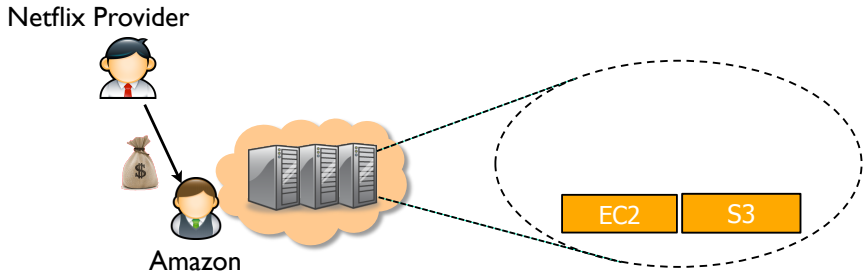


IaaS Example: EC2 and S3



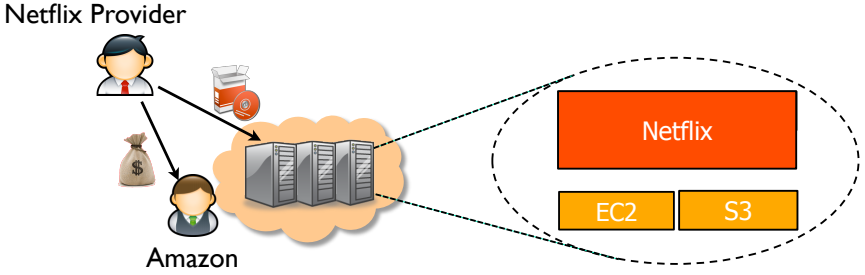
- Netflix (app) heavily depends on Amazon AWS:

IaaS Example: EC2 and S3



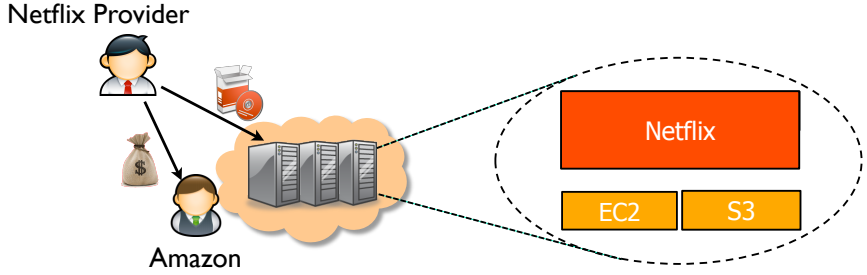
- Netflix (app) heavily depends on Amazon AWS:

IaaS Example: EC2 and S3



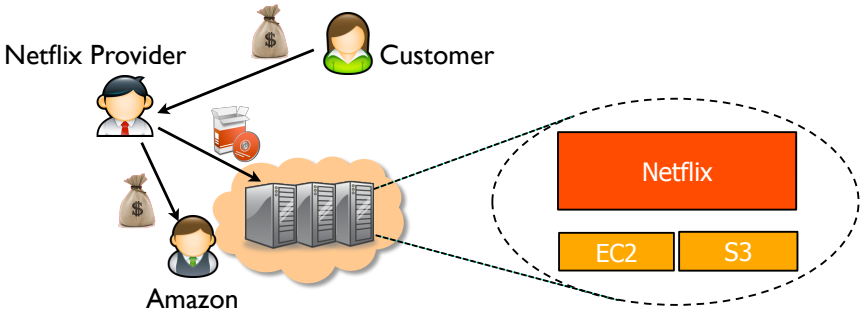
- Netflix (app) heavily depends on Amazon AWS:

IaaS Example: EC2 and S3



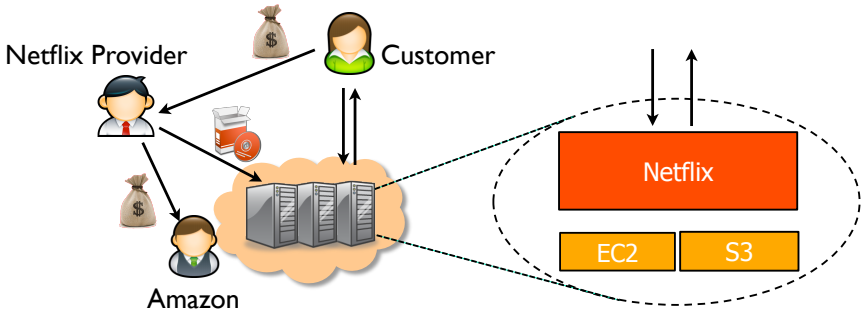
- Netflix (app) heavily depends on Amazon AWS:
  - Media files are stored in S3
  - Transcoding to target devices (e.g., iPad) using EC2

IaaS Example: EC2 and S3



- Netflix (app) heavily depends on Amazon AWS:
  - Media files are stored in S3
  - Transcoding to target devices (e.g., iPad) using EC2

IaaS Example: EC2 and S3



- Netflix (app) heavily depends on Amazon AWS:
  - Media files are stored in S3
  - Transcoding to target devices (e.g., iPad) using EC2

Types of Cloud Services

- Three types of services:
  - Software as a Service (SaaS)
    - Analogy: Restaurant. Prepares&serves entire meal, does the dishes, etc
  - Platform as a Service (PaaS)
    - Analogy: Take-out food. Prepares meal but does not serve it.
  - Infrastructure as a Service (IaaS)
    - Analogy: Grocery store. Provides raw ingredients.

The Major Cloud Providers

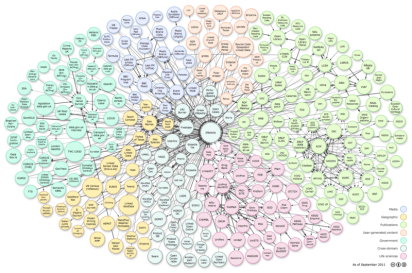
- Amazon is the big player:
  - Infrastructure as a service (e.g., EC2)
  - Storage as a service (e.g., S3)

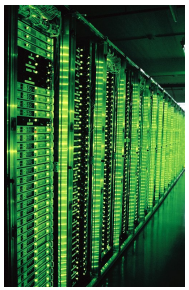
The Major Cloud Providers

- Amazon is the big player:
  - Infrastructure as a service (e.g., EC2)
  - Storage as a service (e.g., S3)
- But there are many others:
  - Microsoft Azure: It has similar services to Amazon, with an emphasis on .Net programming model
  - Google App Engine: It offers programming interface, Hadoop, also software as a service, e.g., Gmail and Google Docs
  - IBM, HP, Yahoo!: They seem to focus on enterprise scale cloud apps

Challenges?

In the cloud, we have much more data and users than before





Data! Users! Traffic!

PC

Server

Cluster

Data center

- What if cluster is too big to fit into machine room?
  - Build a separate building for the cluster
  - Building can have lots of cooling and power
  - Result: Data center

Google's Datacenter in Oregon

Data centers (size of a football field)

- A warehouse-sized computer
  - A single data center can easily contain 10,000 racks with 100 cores in each rack (1,000,000 cores total)

Google's Datacenter Locations

Challenges?

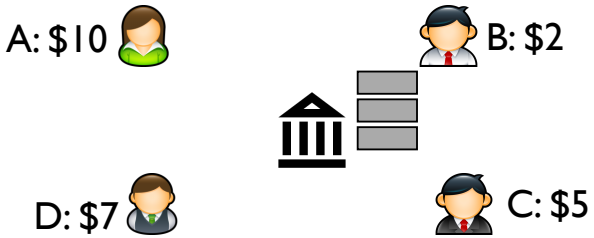
- How to manage a huge group of data?
  - How to store the data?
  - How to process and extract something from the data?
  - How to handle multiple availability and consistency?
  - How to preserve the data privacy?

Example: Google

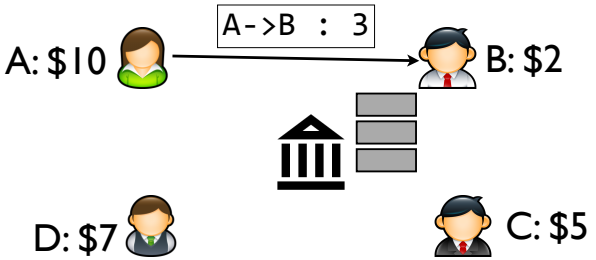
- How to manage a huge group of data?
  - How to store the data? Google File System & BigTable
  - How to process and extract something fro MapReduce
  - How to handle multiple ava Paxos onsistency?
  - How to preserve the data privacy?

BitCoin ≠ Blockchain

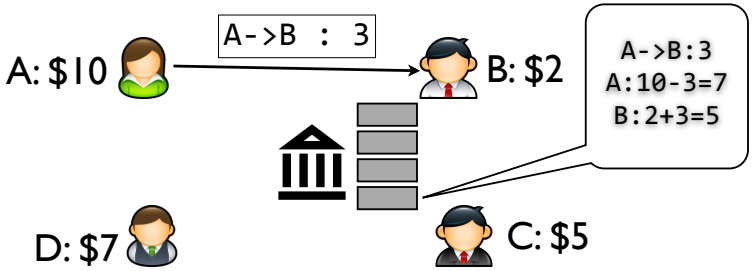
The Blockchain



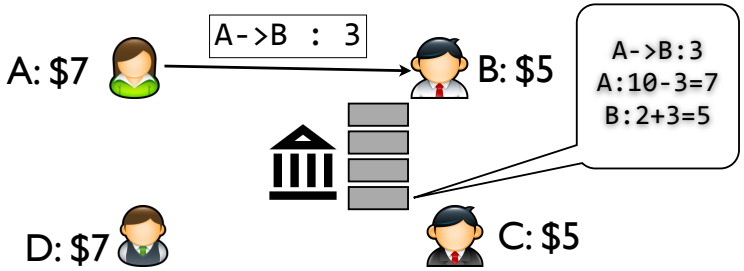
The Blockchain



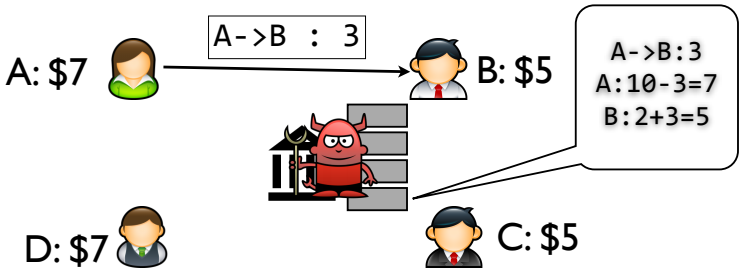
The Blockchain



The Blockchain

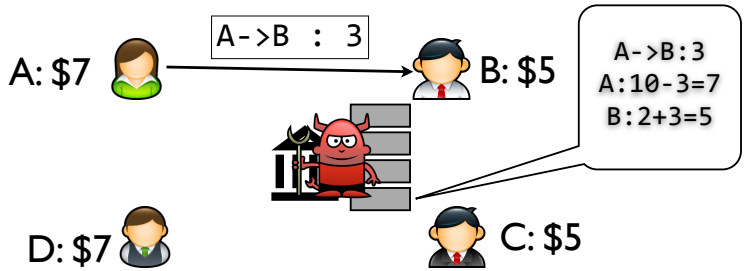


The Blockchain



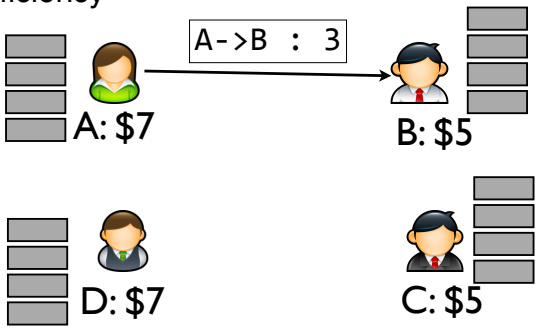
The Blockchain

- Blockchain is used to decentralize the log:



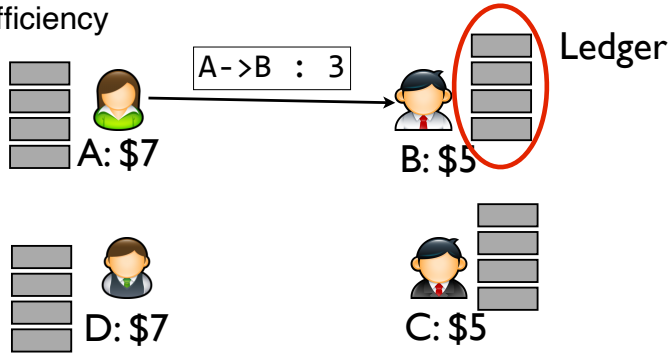
The Blockchain

- Blockchain is used to decentralize the log:
  - Decentralization
  - Public accountability
  - Efficiency



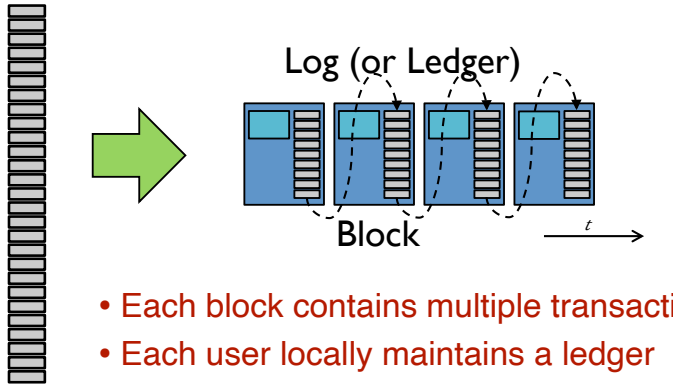
The Blockchain

- Blockchain is used to decentralize the log:
  - Decentralization
  - Public accountability
  - Efficiency



The Blockchain

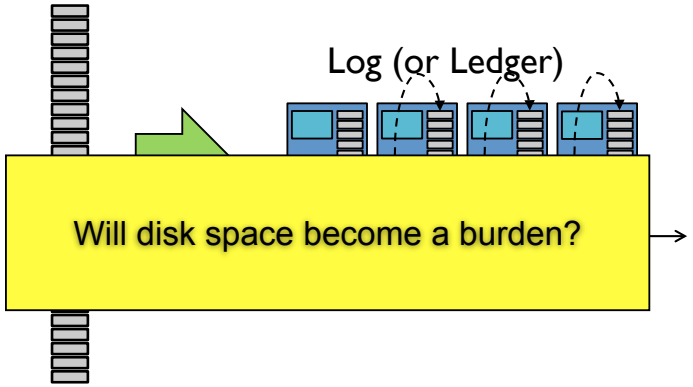
Log (or Ledger)



- Each block contains multiple transactions
- Each user locally maintains a ledger
- All ledgers should have the same data

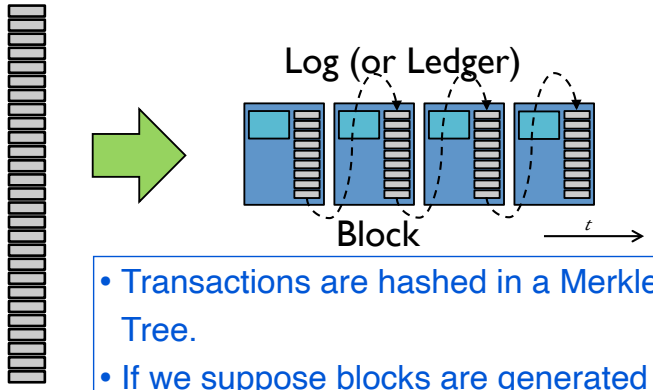
The Blockchain

Log (or Ledger)



The Blockchain

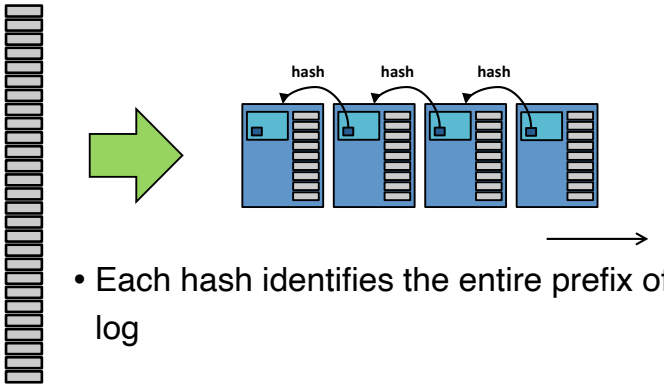
Log (or Ledger)



- Transactions are hashed in a Merkle Tree.
- If we suppose blocks are generated every 10 minutes, then 4.2MB per year.

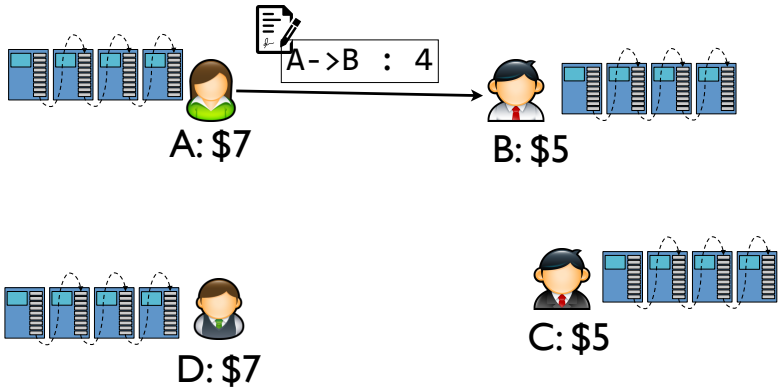
The Blockchain

Log (or Ledger)

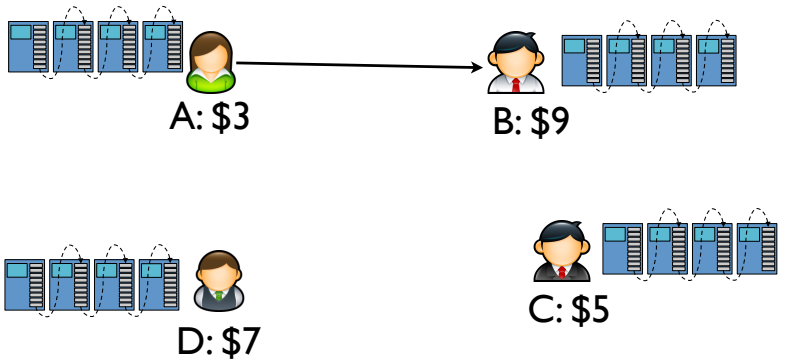


- Each hash identifies the entire prefix of the log

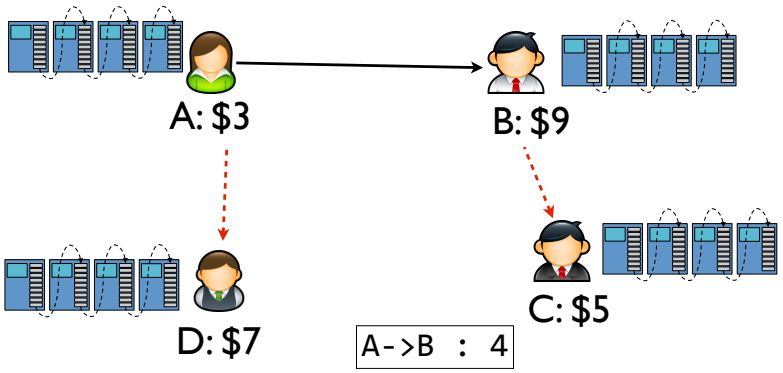
Transactions in the Blockchain



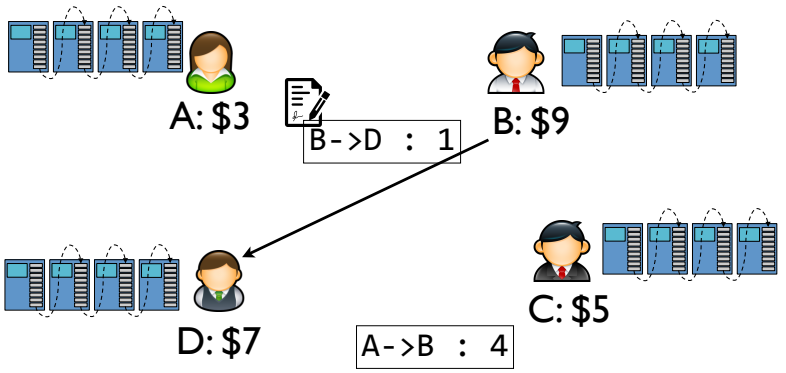
Transactions in the Blockchain



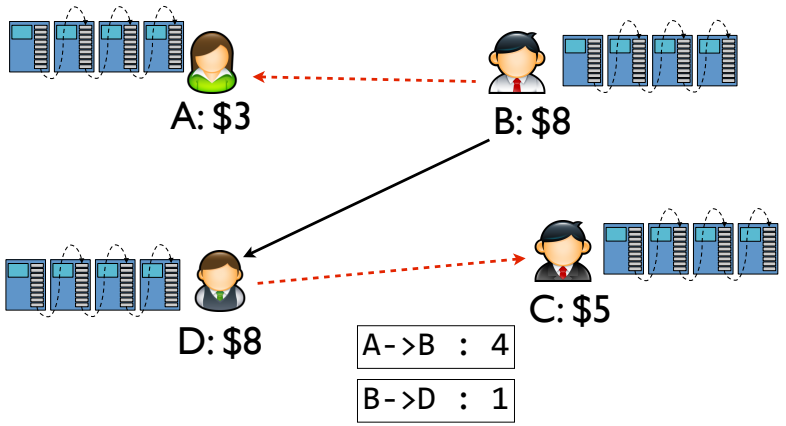
Transactions in the Blockchain



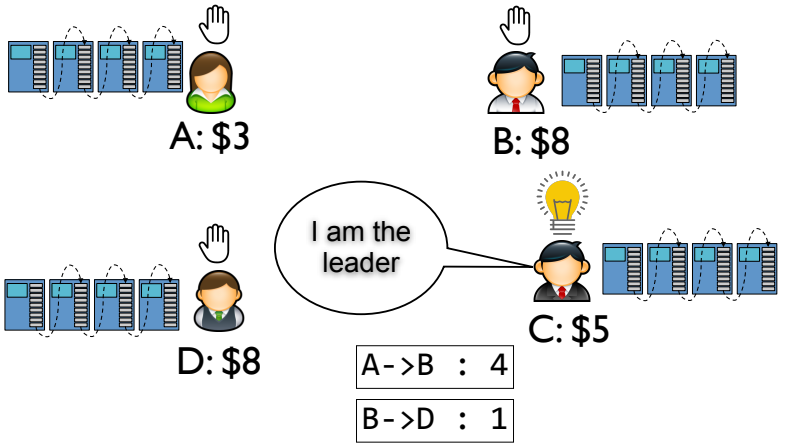
Transactions in the Blockchain



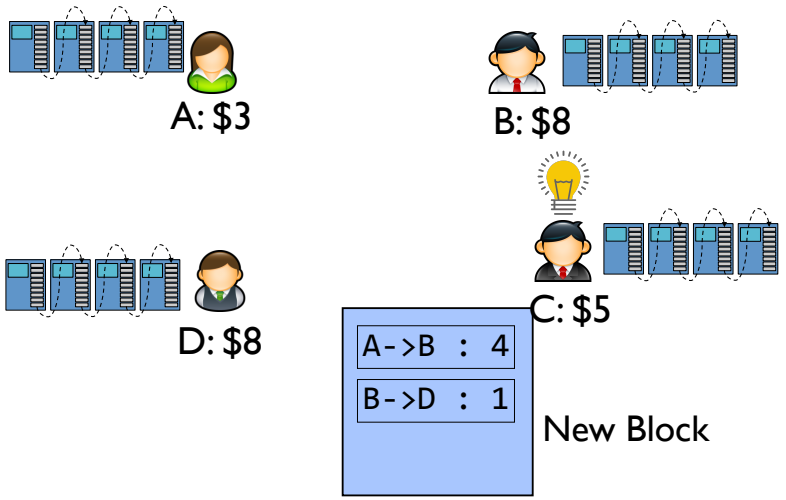
Transactions in the Blockchain



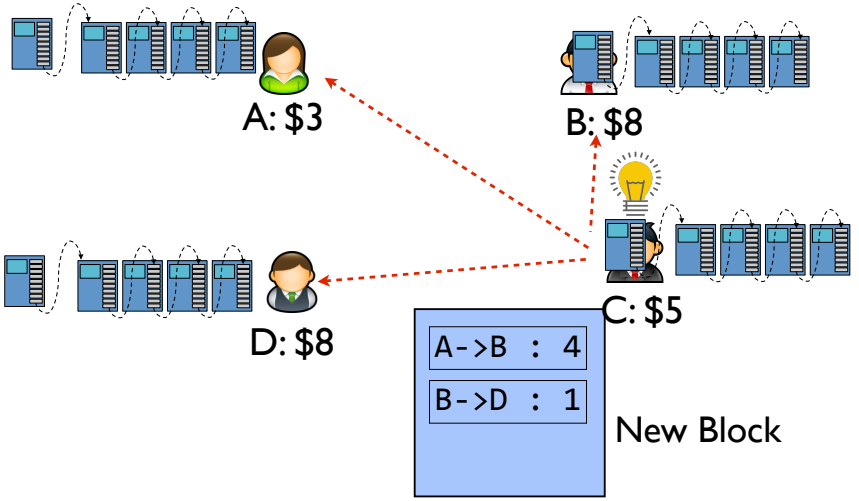
Consensus



New Block Generation



New Block Generation



The Blockchain

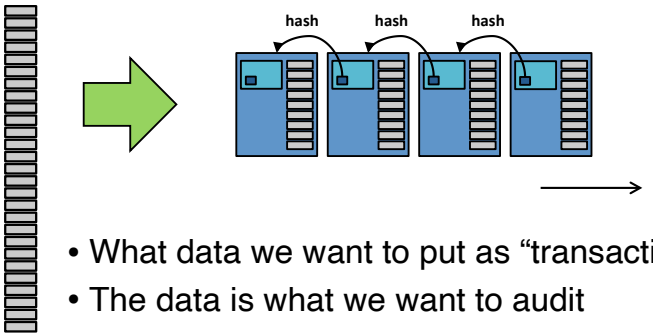
- Blockchain can be used to decentralize any centralized service:
  - Making them decentralized (without single-point-fault)
  - Public accountability

The Blockchain

- Blockchain can be used to decentralize any centralized service:
  - Making them decentralized (without single-point-fault)
  - Public accountability
- We still have two problems:
  - How to achieve consensus?
  - How to preserve the privacy?

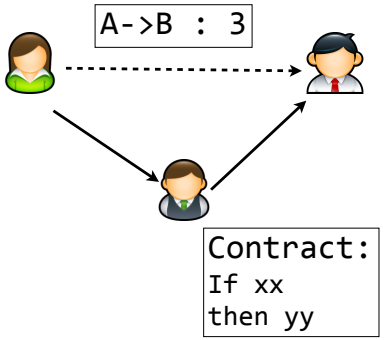
How to decentralize app via blockchain?

Log (or Ledger)

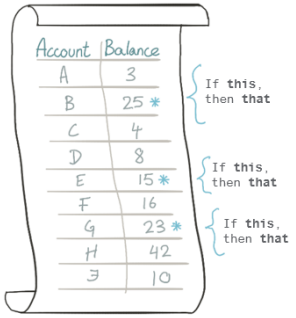


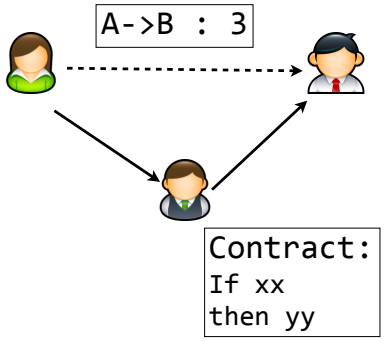
- What data we want to put as “transaction”
- The data is what we want to audit

Smart Contract



Smart Contract





Example

- You are planning to ship a laptop to your friend Bob
  - You trust Bob, but you do not trust trucker Tom
  - Tom will carry your laptop
  - Tom does not trust since maybe you will not pay him

Example

- You are planning to ship a laptop to your friend Bob
  - You trust Bob, but you do not trust trucker Tom
  - Tom will carry your laptop
  - Tom does not trust since maybe you will not pay him

You and Tom have to sign a contract.

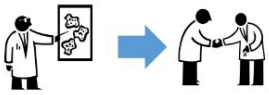
Example

- We can use smart contract:
  - You and Tom define all the rules in code
  - You make a payment for shipment to smart contract on a day of loading.
  - It holds payment till shipment delivery is confirmed by Bob.
  - Smart contract releases the payment and money is transferred to Tom automatically.

Another Example

Doctor informs patient that they need to exercise

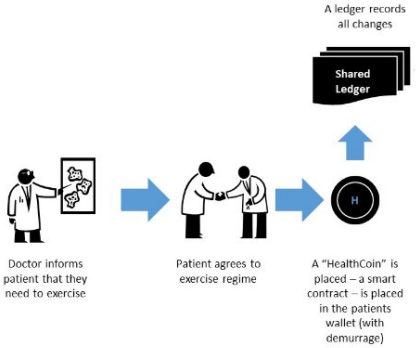
Another Example



Doctor informs patient that they need to exercise

Patient agrees to exercise regime

Another Example

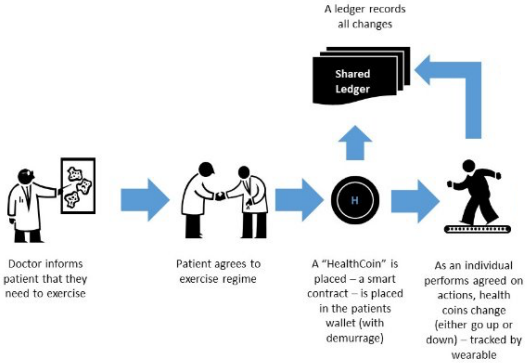


Doctor informs patient that they need to exercise

Patient agrees to exercise regime

A "HealthCoin" is placed – a smart contract – is placed in the patients wallet (with demurrage)

Another Example



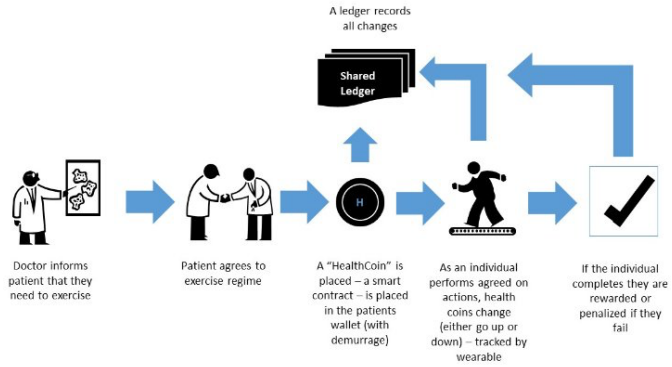
Doctor informs patient that they need to exercise

Patient agrees to exercise regime

A "HealthCoin" is placed – a smart contract – is placed in the patients wallet (with demurrage)

As an individual performs agreed on actions, health coins change (either go up or down) – tracked by wearable

Another Example

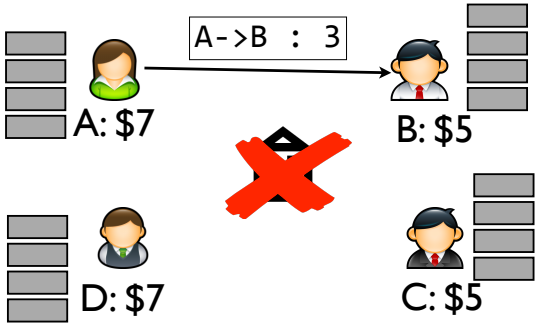


The Blockchain

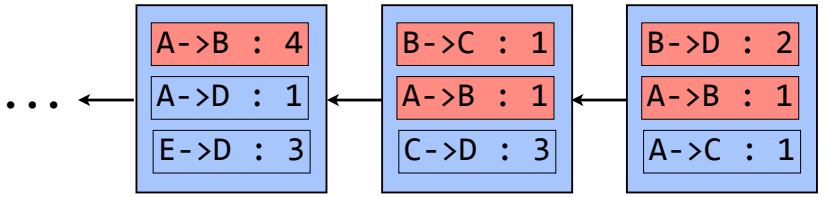
- Blockchain can be used to decentralize any centralized service:
  - Making them decentralized (without single-point-fault)
  - Public accountability
- We still have two problems:
  - How to achieve consensus?
  - How to preserve the privacy?

Deployment of BitCoin Nodes

- Blockchain is used for a decentralized bank:
  - Each user has several wallets (public keys)
  - They sign the money transaction using the private key



How to compute BitCoin?



If B's initial value is 0, then B is 4-1+1-2+1=3

How to compute BitCoin?

Inputs

Previous output (index)	Amount	From address	Type	ScriptSig
eb38f77560ca…:1	8	1P9SgqzjFWgWVAuZBFwimNPV7LauaJpgTj	Address	30450220078df7c48ed152bd40eaee4a73afefc3 044760639da2c0d6158484e1a4dab332fefc4bb
b912994fca58…:1	0.03	18Mk65wV1E5kCVHFShvUTU6zt4yVFKM5Ft	Address	304502204e877fc5ca3783e165052e64c4788dd 04769bbfc55cbd412784e024c8624f8c4f42d7cb
58379d94fe85…:15	1	1G4hfnM2nfAPEECdawg5grvUTBB2PxvLr2	Address	3044022075d23fd4a80048667772 10f51f46c96 046dd45b37fe3ff33f1563458cfbdfb7f922d1b4a
fc9d1cd1c2ac…:1	130	1LpQVnJSMgqqhQBGZwboobdX2Glm9YWyC7	Address	3046022100a65a188b89a4e5ae2eaa5ba387503 04ba81a1a538c5ddf7e0c76884497ab522456b9
7b6f7d4a521c…:1	0.55357267	16Kb6XppHUbjgmYQDpRyxz9JNE9Az5Xvcb	Address	3045022100eeb76e61abe62d38fd462eafd1d11f 04f4fa1d3e26f3e7058038871a31b8bf636fd127f6
544097a30e09…:0	0.03270607	1JnsDx1g6c757z8AnJUemj46YQgCTw54QN	Address	3045022100859df2ced47493e86a849cce10615 04de257fe6490bd16188be6d06ca7b34816fa4b

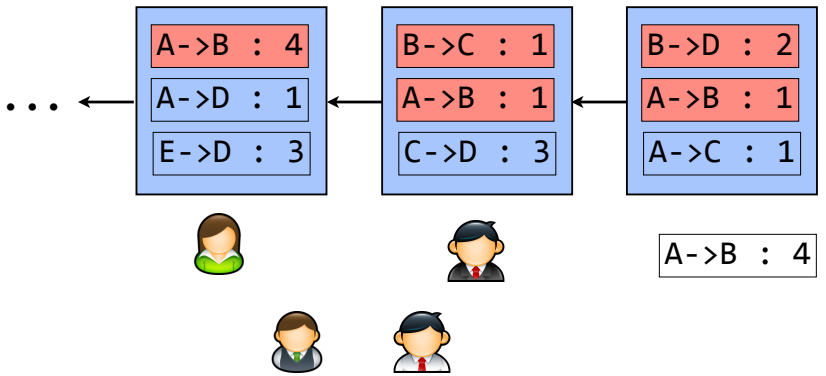
139.6

Outputs

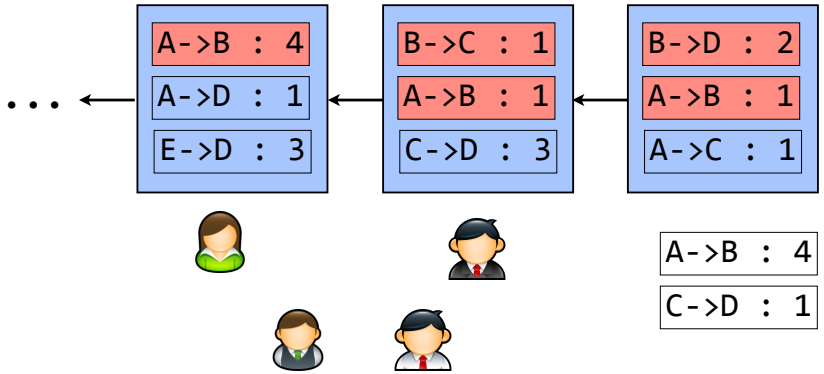
Index	Redeemed at input	Amount	To address	Type	ScriptPubKey
0	8baaca27d158…	0.01071174	1E7BgzQbyWTWzEMUKNrzLdjkbjaQT9K96m	Address	OP_DUP OP_HASH160 9abd2e0c0a63dea36b75c3128fe15d82f274e394 OP_EQUALVERIFY OP_CHECKSIG
1	1bb973b4cce8…	139.605567	1NT2rFMa11NiCZydt4kqgXRZPf3iS6ZPGZ	Address	OP_DUP OP_HASH160 eb471d7a903e538cb94c1f2faf20eaadad8479af OP_EQUALVERIFY OP_CHECKSIG

139.6

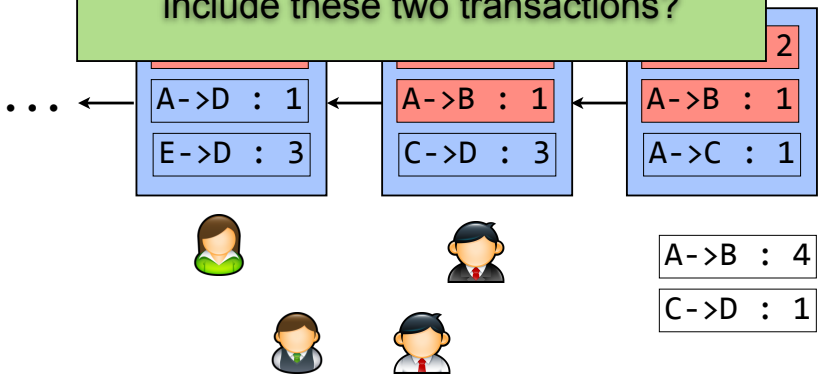
How to compute BitCoin?

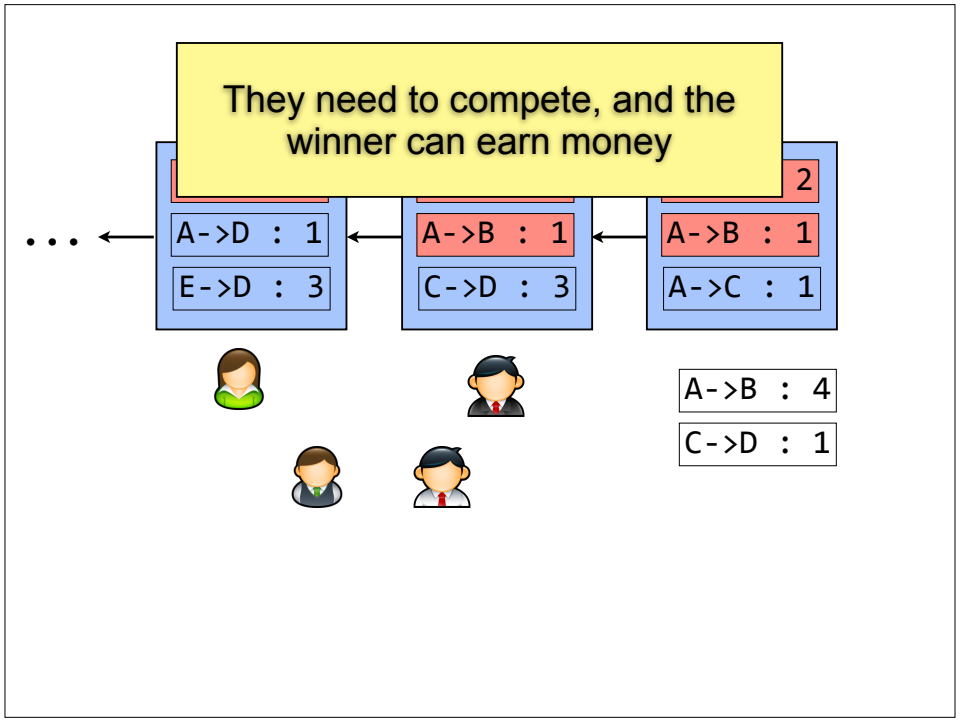


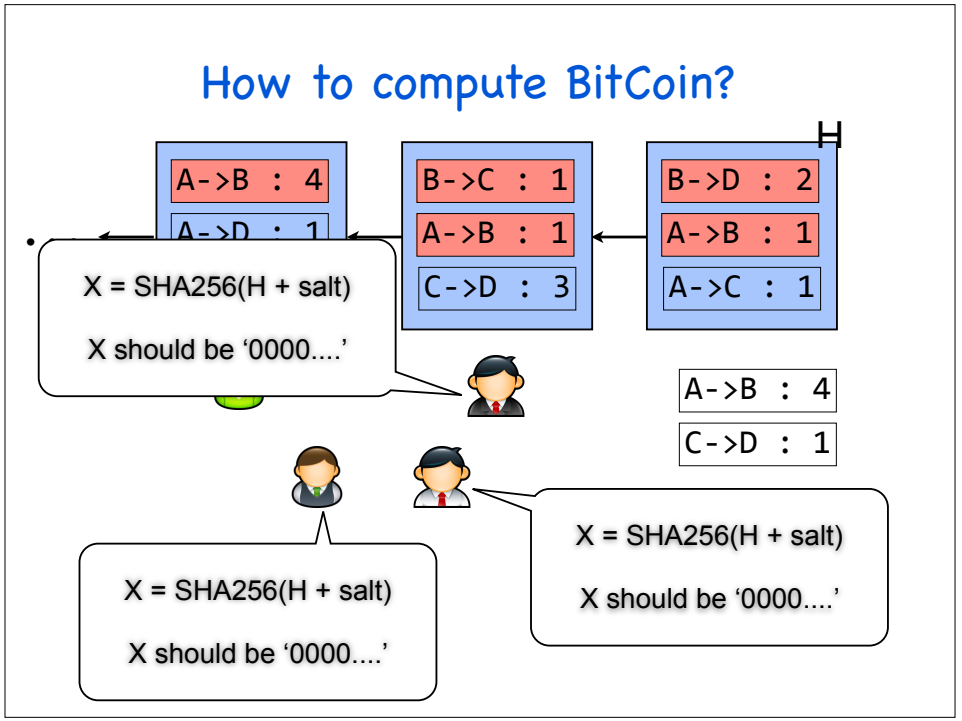
How to compute BitCoin?

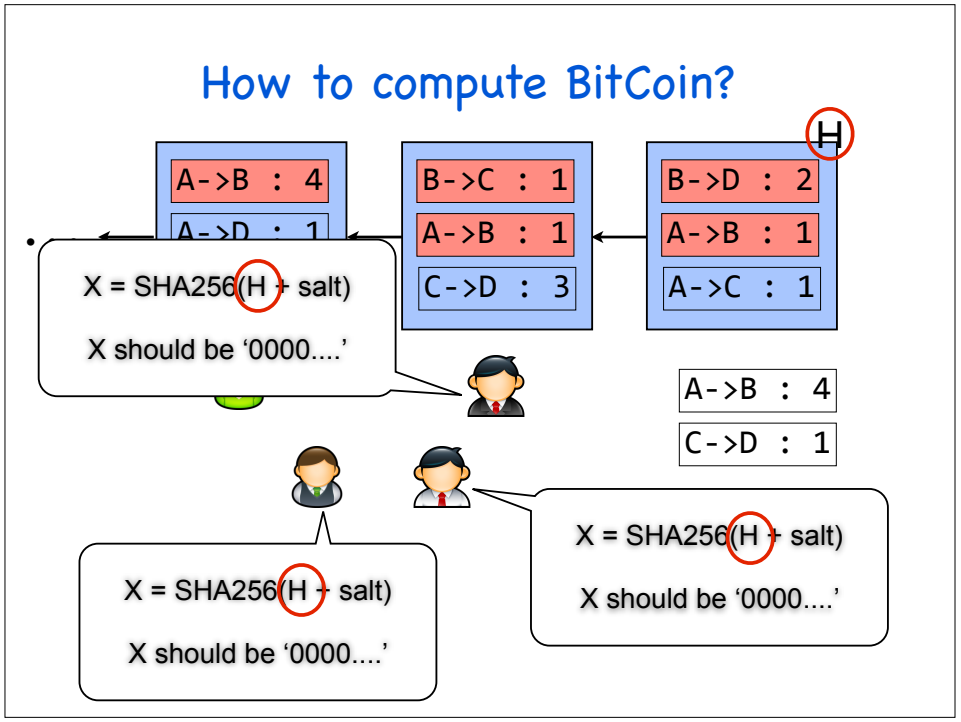


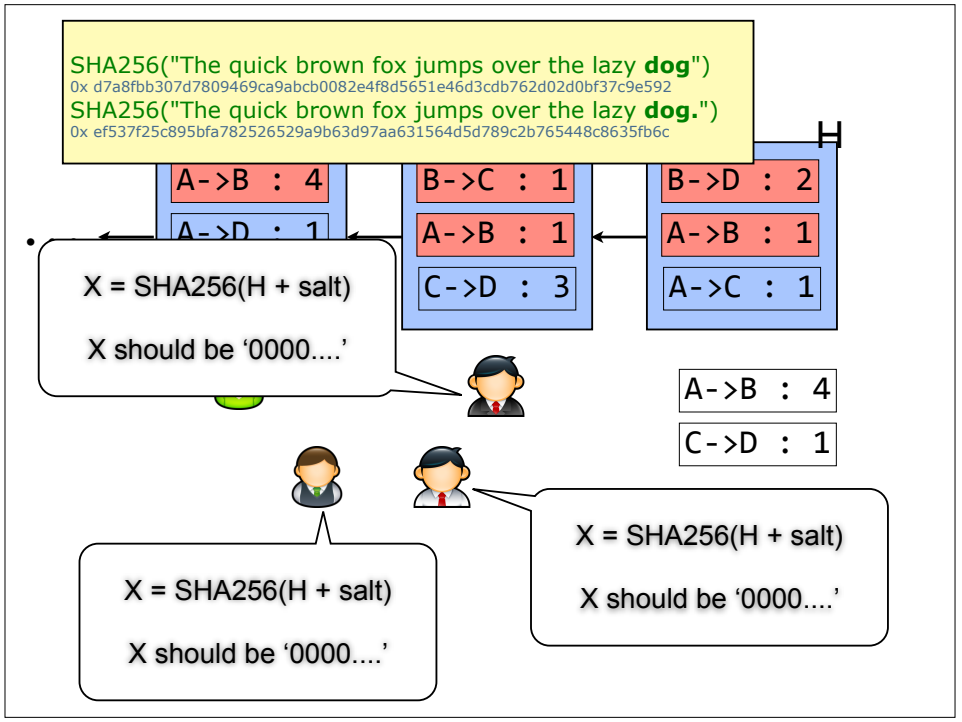
Who should generate a new block to include these two transactions?

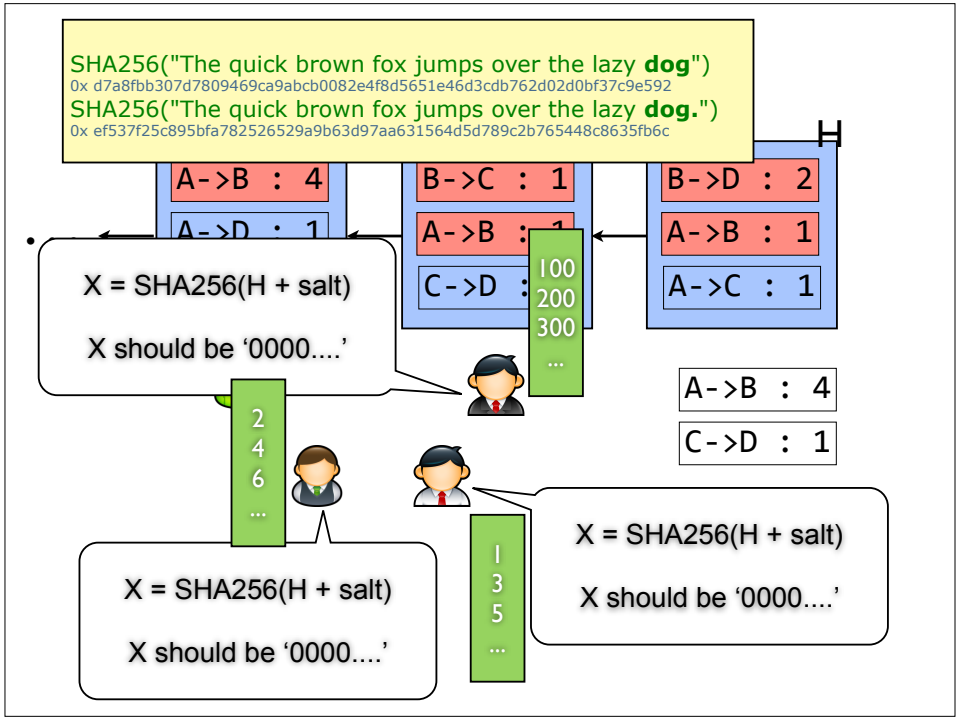


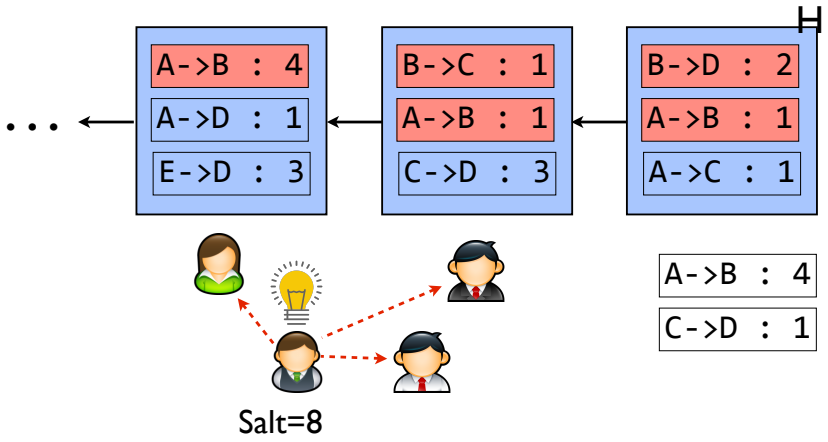

They need to compete, and the winner can earn money
A->D : 1
E->D : 3
A->B : 1
C->D : 3
A->B : 1
A->C : 1
A->B : 4
C->D : 1

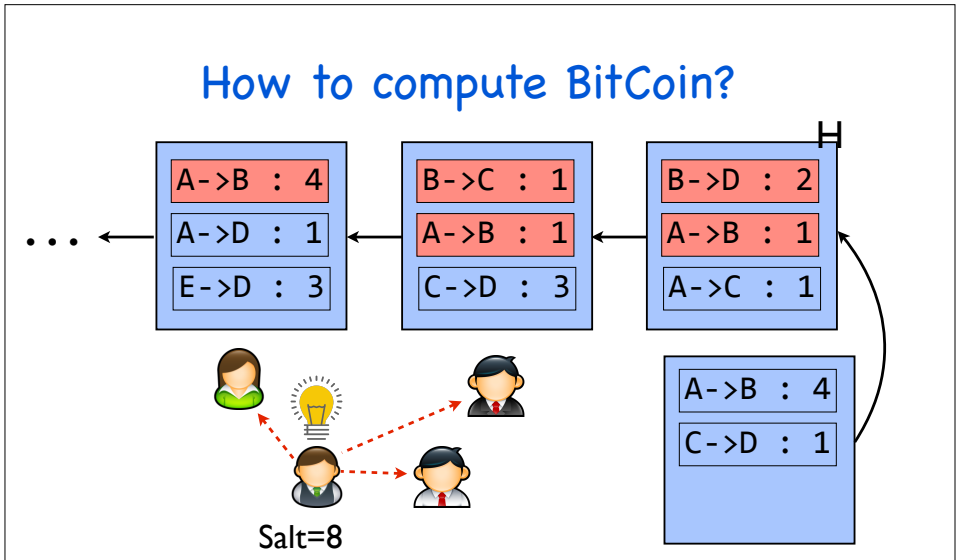

How to compute BitCoin?
H
A->B : 4
B->C : 1
A->B : 1
C->D : 3
B->D : 2
A->B : 1
A->C : 1
X = SHA256(H + salt)
X should be '0000....'
A->B : 4
C->D : 1
X = SHA256(H + salt)
X should be '0000....'
X = SHA256(H + salt)
X should be '0000....'


How to compute BitCoin?
H
A->B : 4
B->C : 1
A->B : 1
C->D : 3
B->D : 2
A->B : 1
A->C : 1
X = SHA256(H + salt)
X should be '0000....'
A->B : 4
C->D : 1
X = SHA256(H + salt)
X should be '0000....'
X = SHA256(H + salt)
X should be '0000....'


SHA256("The quick brown fox jumps over the lazy dog")
0x d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592
SHA256("The quick brown fox jumps over the lazy dog.")
0x ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c
H
A->B : 4
B->C : 1
A->B : 1
C->D : 3
B->D : 2
A->B : 1
A->C : 1
X = SHA256(H + salt)
X should be '0000....'
A->B : 4
C->D : 1
X = SHA256(H + salt)
X should be '0000....'
X = SHA256(H + salt)
X should be '0000....'







Proof of Work

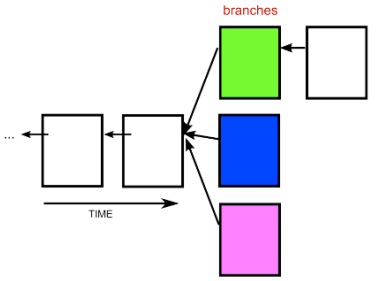
- BitCoin uses the proof of work to achieve many goals:
  - Generating additional money
  - Achieving consensus while tolerating malicious users
  - A great incentive mechanism

Proof of Work

- BitCoin uses the proof of work to achieve many goals:
  - Generating additional money
  - Achieving consensus while tolerating malicious users
  - A great incentive mechanism

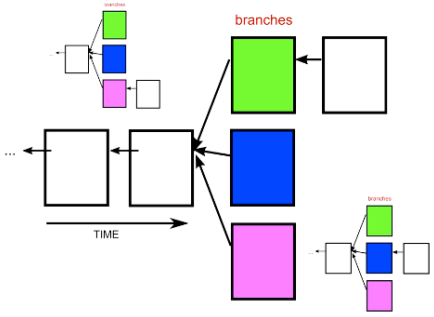
Proof of Work

- Occasionally, more than one block will be solved at the same time, leading to several possible branches



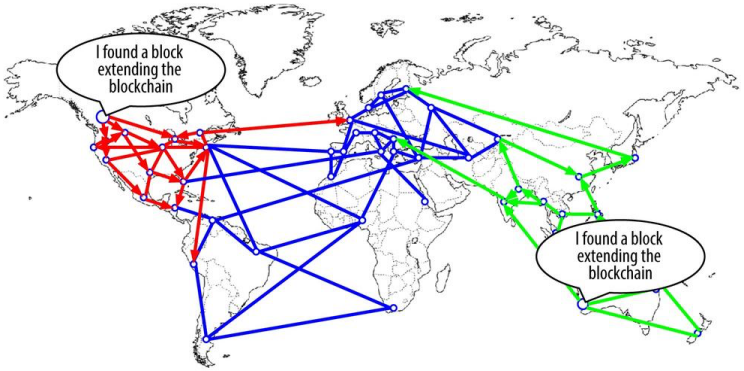
Proof of Work

- We should build on top of the first one you received.
- Others may have received the blocks in a different order, and will be building on the first block they received

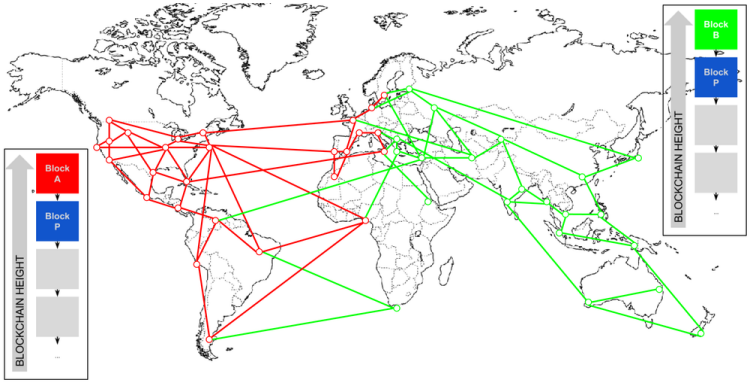


Example

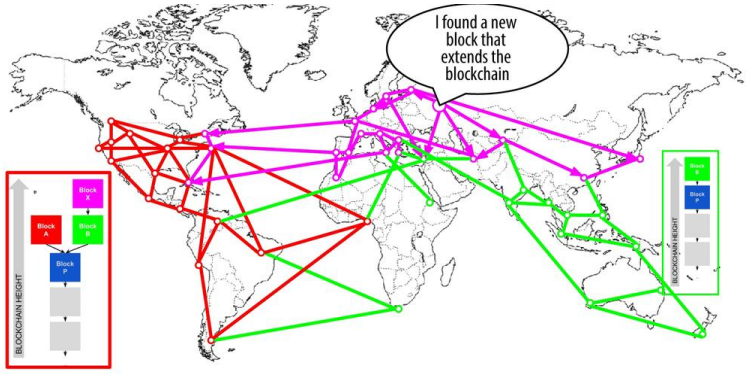
Example



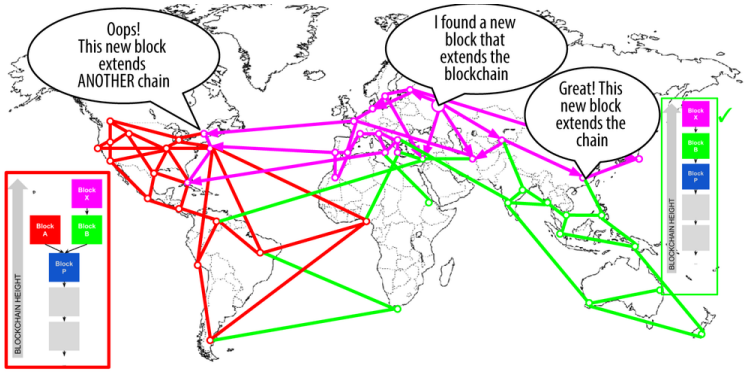
Example



Example



Example



Proof of Work

- We do not need to worry about the branch problem:
  - You always immediately switch to the longest branch
  - The math makes it rare for blocks to be solved at the same time, and even more rare for this to happen multiple times
  - The end result is the block chain quickly stabilizes

Proof of Work

- We do not need to worry about the branch problem:
  - You always immediately switch to the longest branch
  - The math makes it rare for blocks to be solved at the same time, and even more rare for this to happen multiple times
  - The end result is the block chain quickly stabilizes
- ~10 minutes to generate a new block
- Your transactions are confirmed after 6 blocks

Proof of Work

- We do not need to worry about the branch problem:
  - You always immediately switch to the longest branch
  - The math makes it rare for blocks to be solved at the same time, and even more rare for this to happen multiple times
  - The end result is the block chain quickly stabilizes

Miners in BitCoin can earn a lot of money!

- ~10 minutes to generate a new block
- Your transactions are confirmed after 6 blocks

Miner's life