Lecture #1: Mental Models for Blockchain Protocols and Web3

COMS 4995-001:
The Science of Blockchains

URL: https://timroughgarden.org/s25/

Tim Roughgarden

Goals for Lecture #1

1. Mental models for blockchain protocols and Web3.
   - i.e., what the technology is trying to achieve
   - answer: the general-purpose functionality of a computer, but with the "decentralization" and "openness" of the Internet
2. Overview of course and its requirements.
   - high-level syllabus, deliverables, etc.

Mental Model for Blockchains/Web3

1. General-purpose functionality of a computer.

Mental Model for Blockchains/Web3

1. General-purpose functionality of a computer.
2. “Decentralization” of the Internet.
   - i.e., no one owner or operator

Mental Model for Blockchains/Web3

1. General-purpose functionality of a computer.
2. “Decentralization” of the Internet.
   - i.e., no one owner or operator

Internet: shared global infrastructure for *communication*.

Mental Model for Blockchains/Web3

1. General-purpose functionality of a computer.
2. “Decentralization” of the Internet.
   - i.e., no one owner or operator

Internet: shared global infrastructure for *communication*.

Blockchain protocol: shared global infrastructure for *computation*.

Mental Model for Blockchains/Web3

1. General-purpose functionality of a computer.

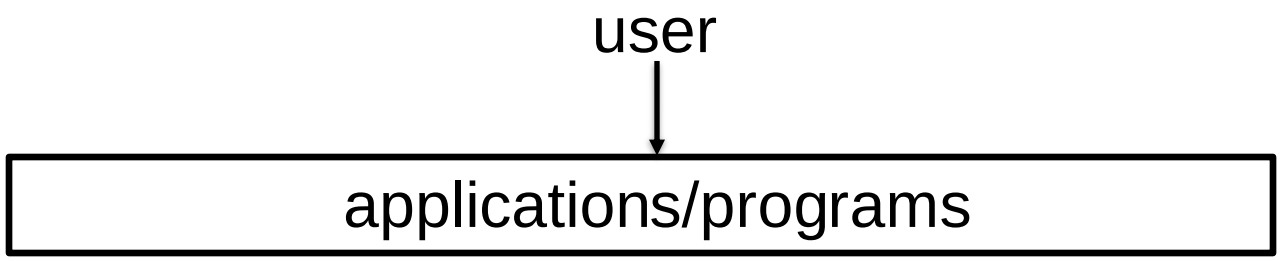
2. "Decentralization" of the Internet.
   - i.e., no one owner or operator

Internet: shared global infrastructure for *communication*.

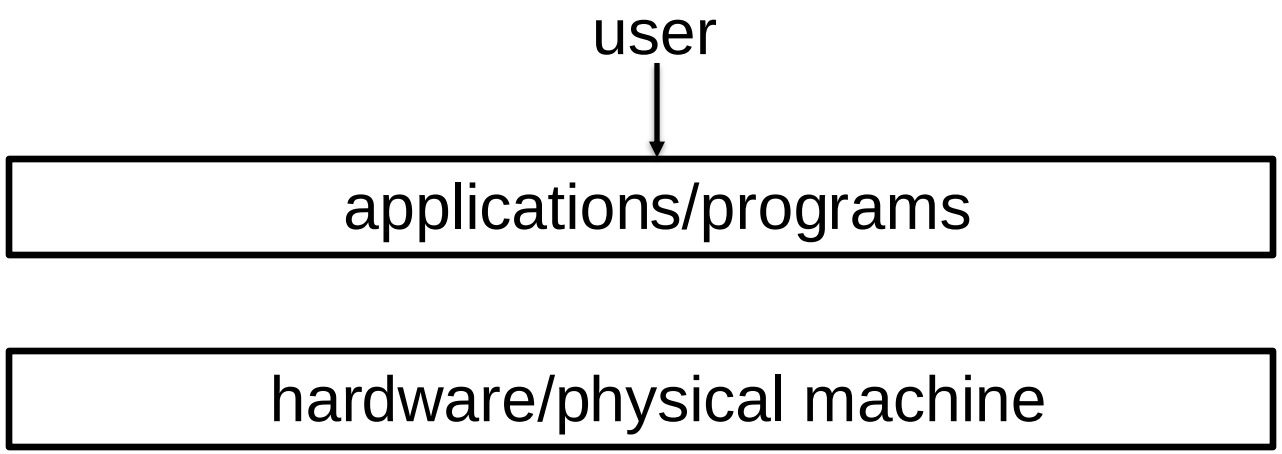
Blockchain protocol: shared global infrastructure for *computation*.

Example application: meaningful ownership of digital assets.
   - narrow gap in property rights for what you buy or create in the digital realm versus in the physical realm

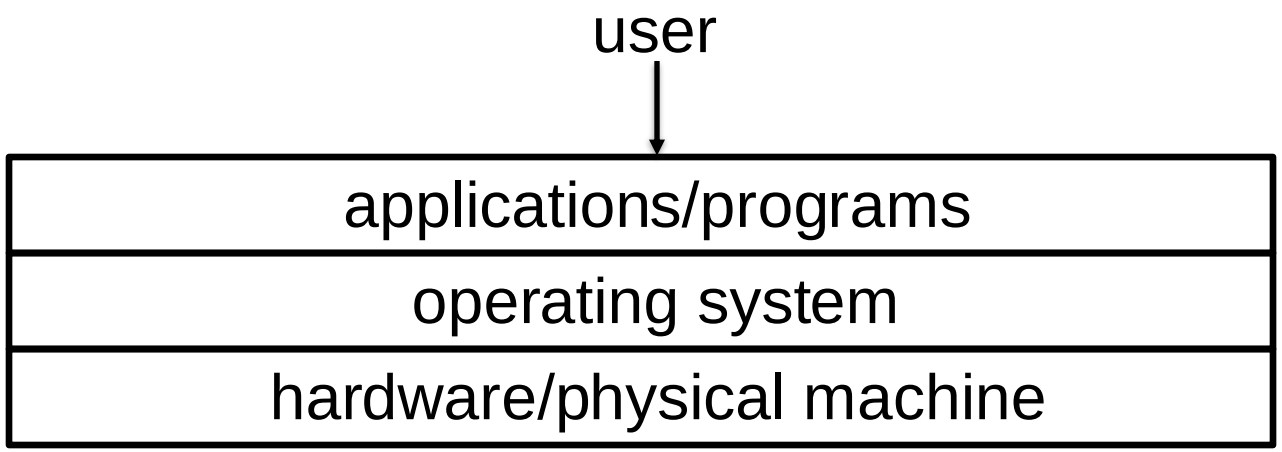
A Cartoon of a Computer



A Cartoon of a Computer



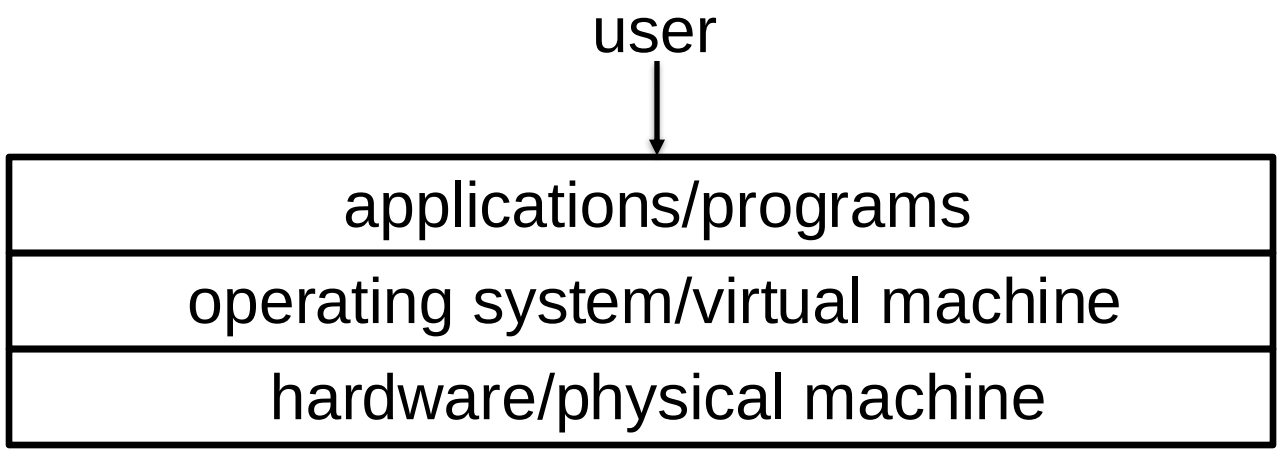
A Cartoon of a Computer



Operating system:

- acts as a “master program” that coordinates all applications

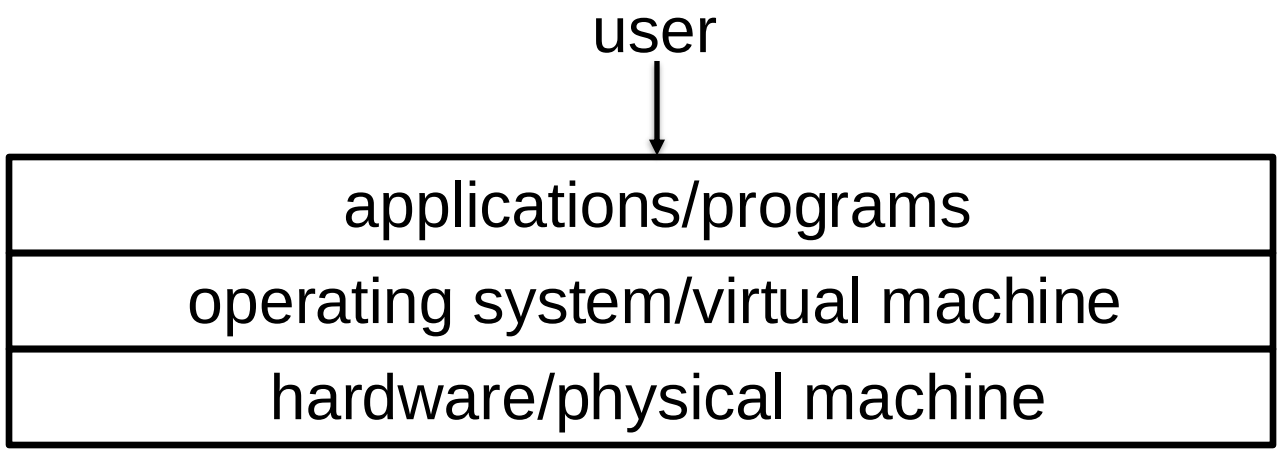
A Cartoon of a Computer



Operating system:

- acts as a “master program” that coordinates all applications
- provides a “virtual machine” to applications
  - applications translate user wants into low-level VM instructions
  - OS ensures that VM instructions realized on the actual hardware

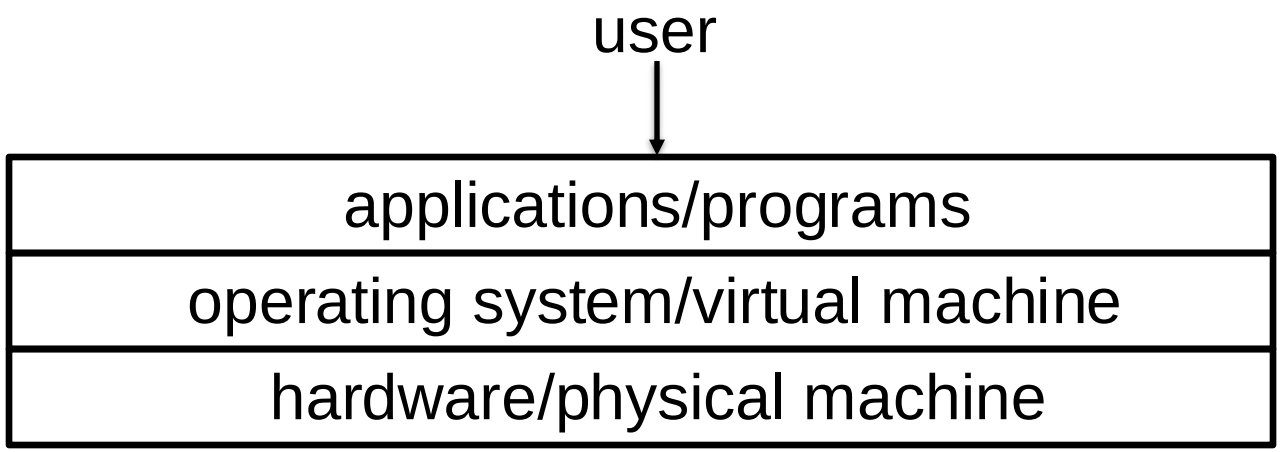
A Cartoon of a Computer



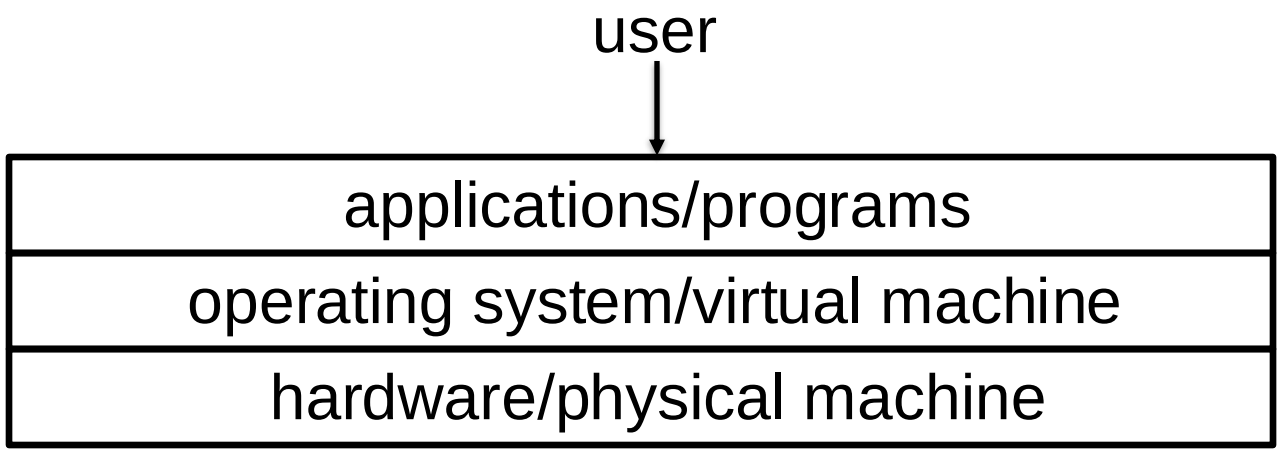
Operating system:

- acts as a “master program” that coordinates all applications
- provides a “virtual machine” to applications
- OS insulates applications from hardware details + vice versa

A Cartoon of a Computer

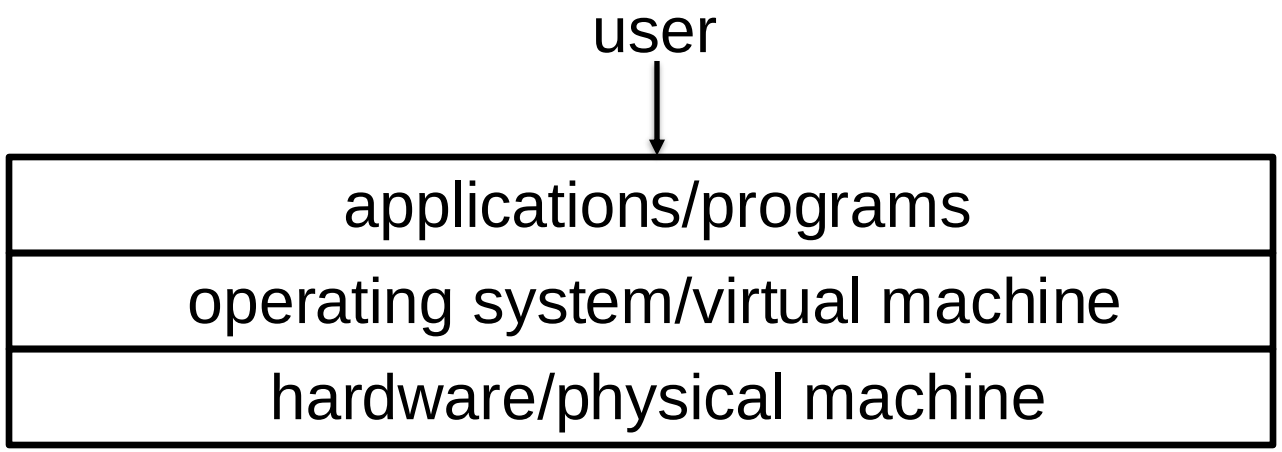


A Cartoon of a Computer



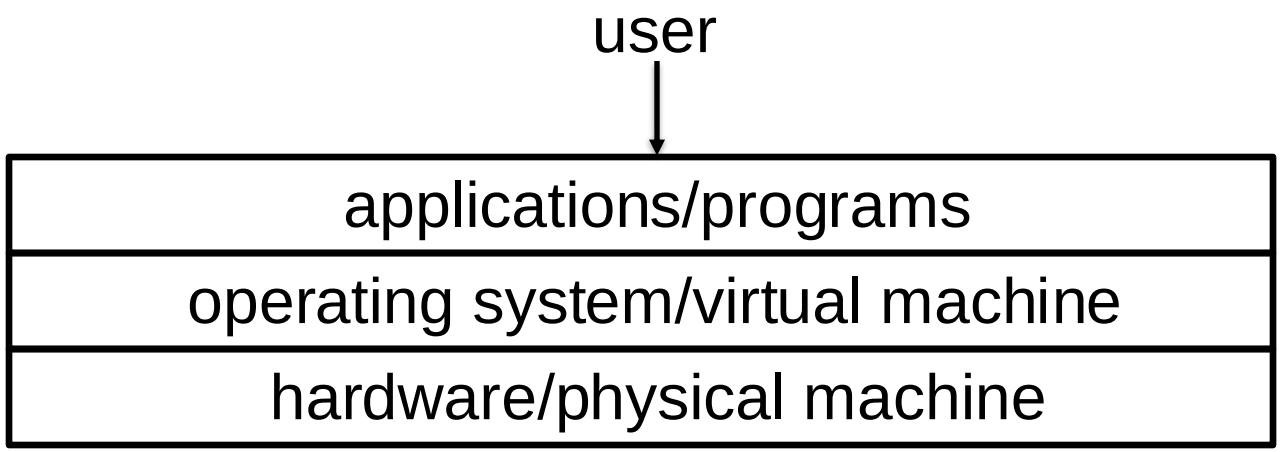
Recall litmus test: does this technology enable meaningful ownership of digital assets?

A Cartoon of a Computer



Good news: capable of any computation.

A Cartoon of a Computer

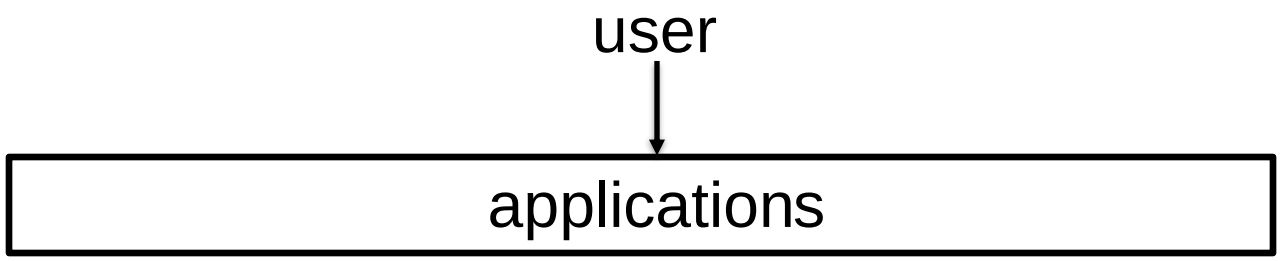


Good news: capable of any computation.

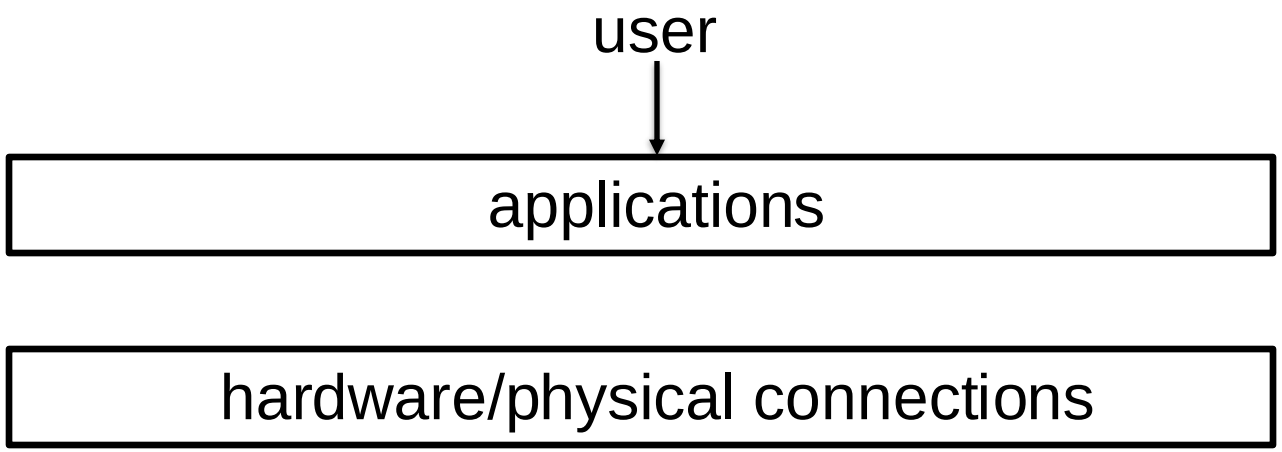
Bad news: neither decentralized nor shared.

- e.g., can't be used for meaningful ownership of digital assets

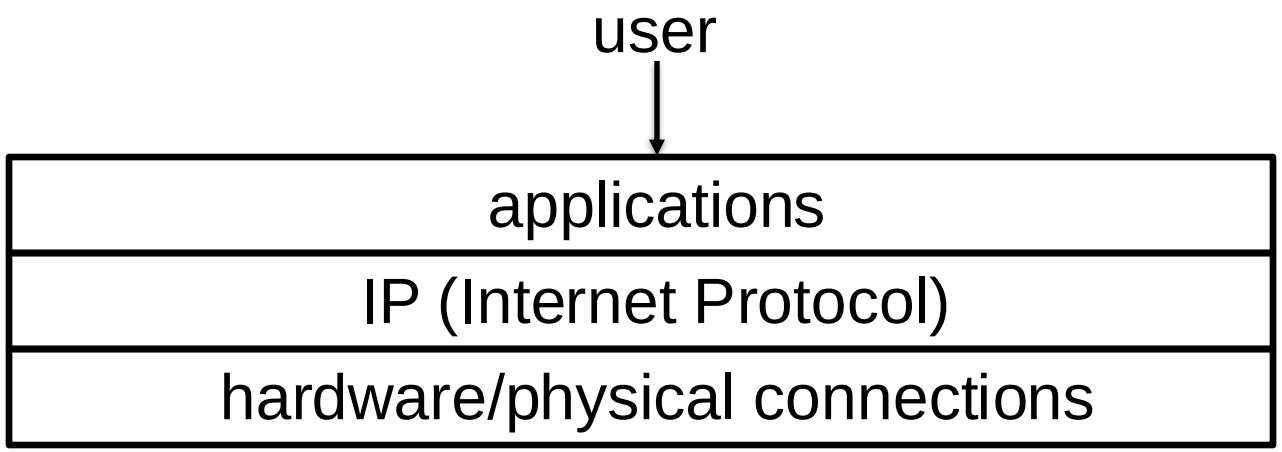
A Cartoon of the Internet



A Cartoon of the Internet



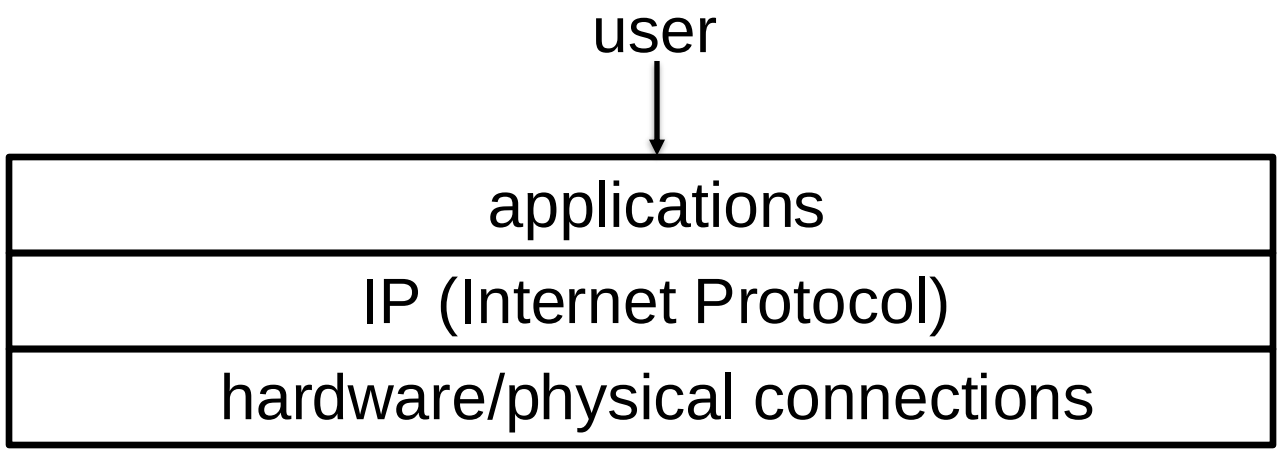
A Cartoon of the Internet



Internet Protocol (IP): provides point-to-point communication.

- insulates applications from low-level network details + vice versa

A Cartoon of the Internet

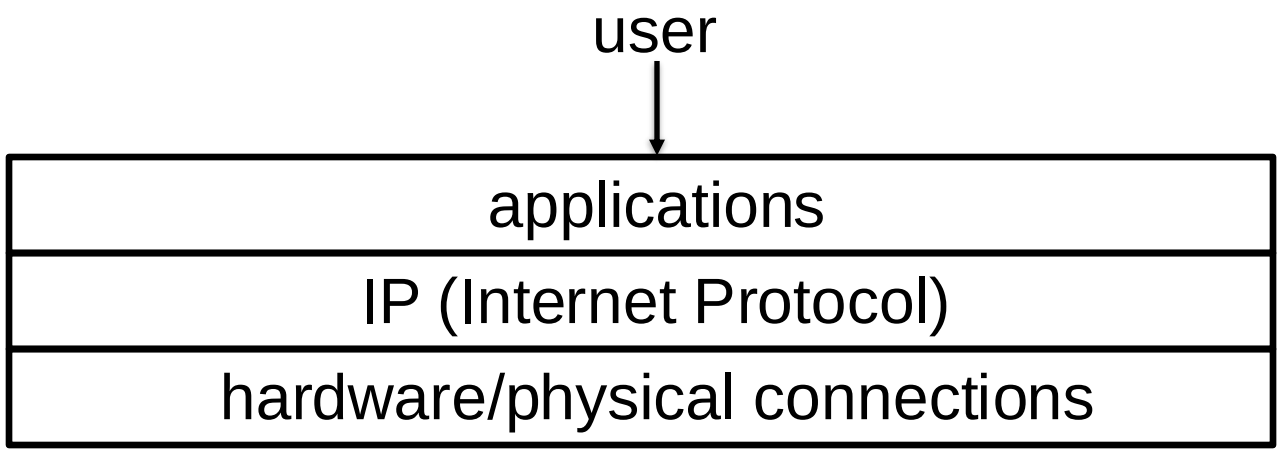


Internet Protocol (IP): provides point-to-point communication.

- insulates applications from low-level network details + vice versa

Recall litmus test: does this technology enable meaningful ownership of digital assets?

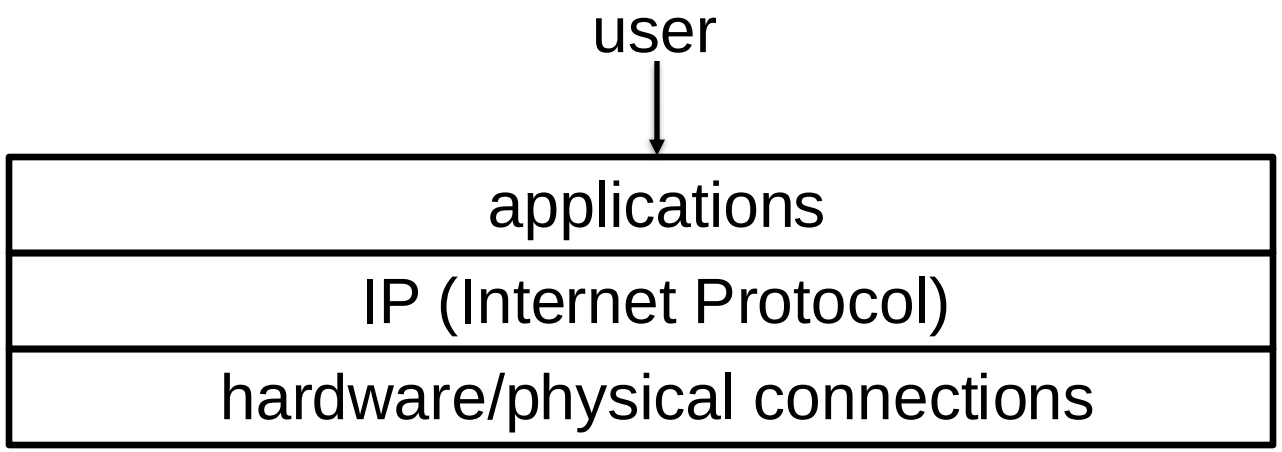
A Cartoon of the Internet



Internet Protocol (IP): provides point-to-point communication.

Good news: shared and “decentralized.”

A Cartoon of the Internet



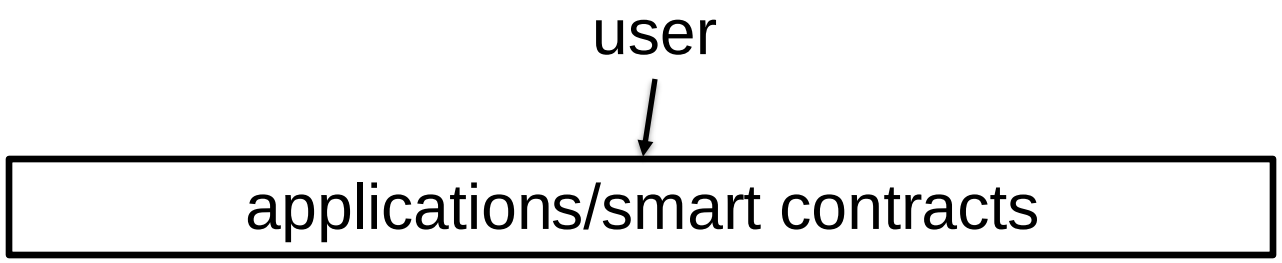
Internet Protocol (IP): provides point-to-point communication.

Good news: shared and “decentralized.”

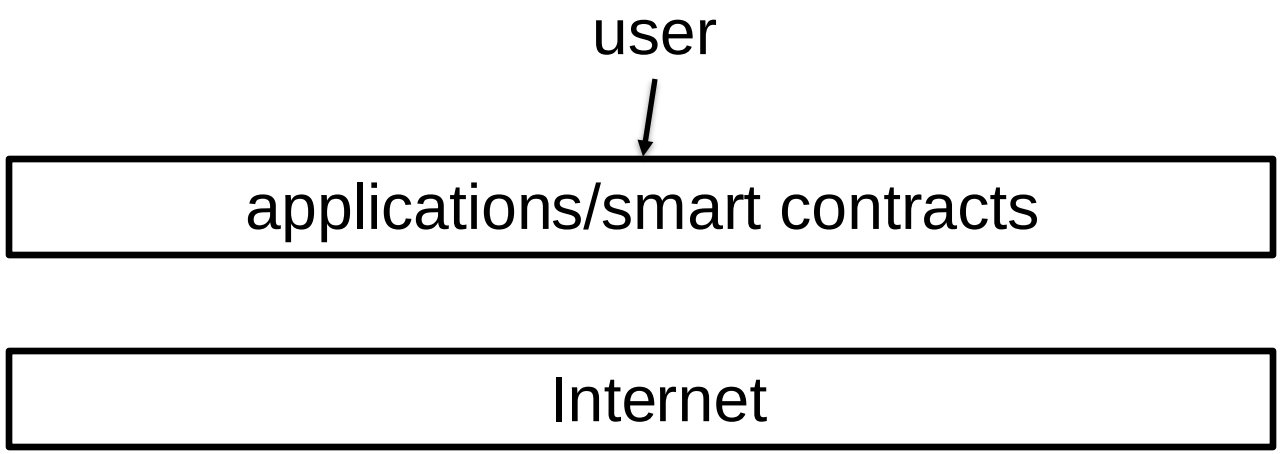
Bad news: only moves bits around (“stateless”).

- can’t be used for meaningful ownership of digital assets

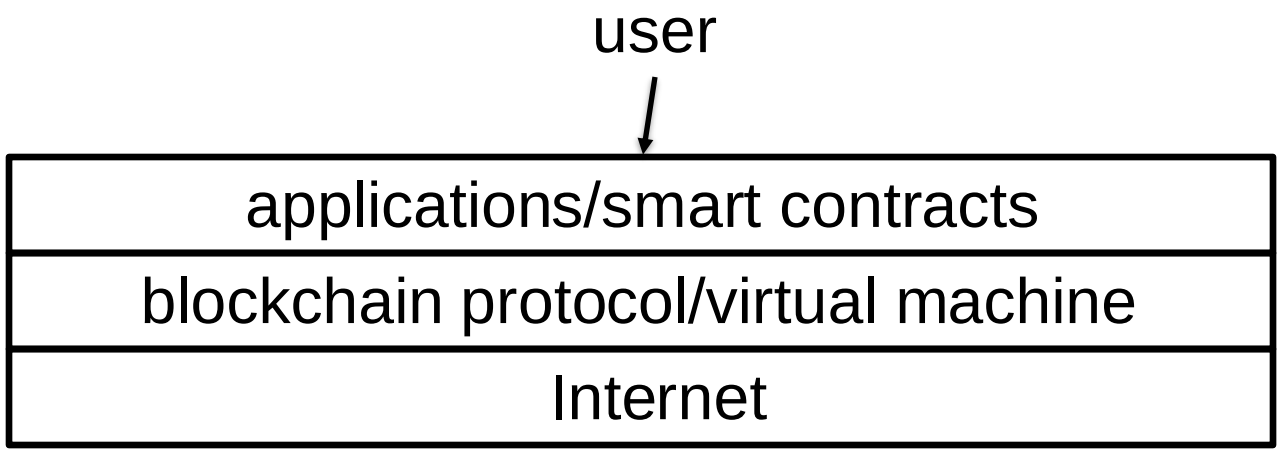
A Cartoon of Web3



A Cartoon of Web3



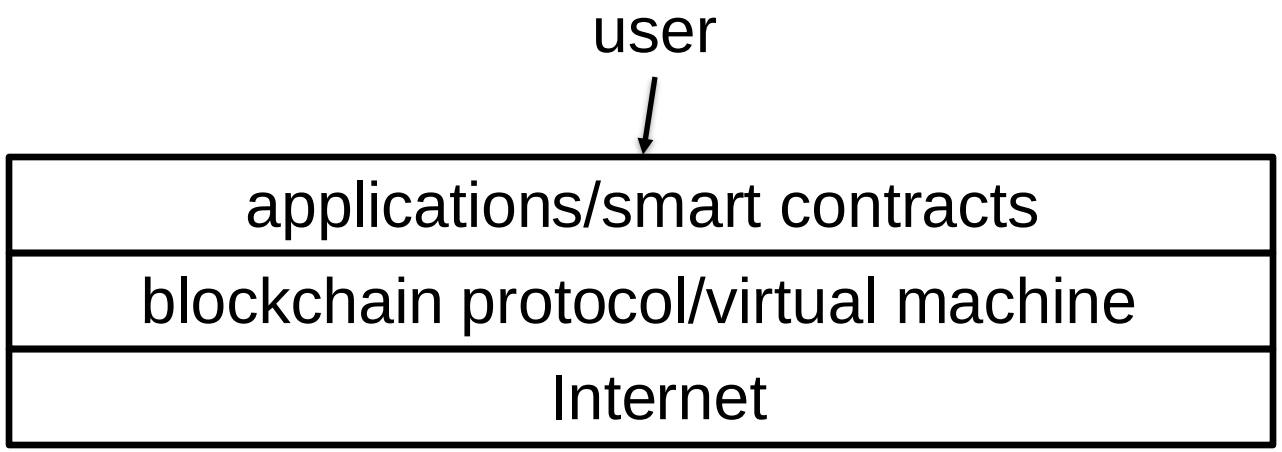
A Cartoon of Web3



Blockchain protocol:

- like an operating system, a blockchain protocol:
  - acts as a “master program” to coordinate all apps/smart contracts
  - provides a virtual machine to developers of applications

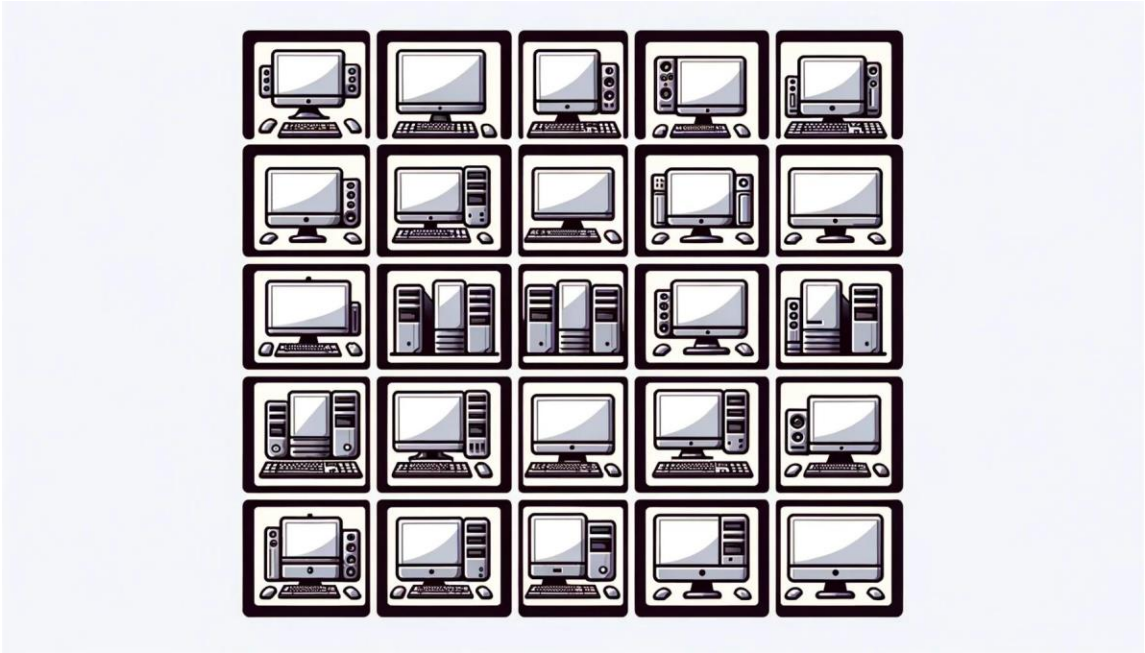
A Cartoon of Web3



Blockchain protocol:

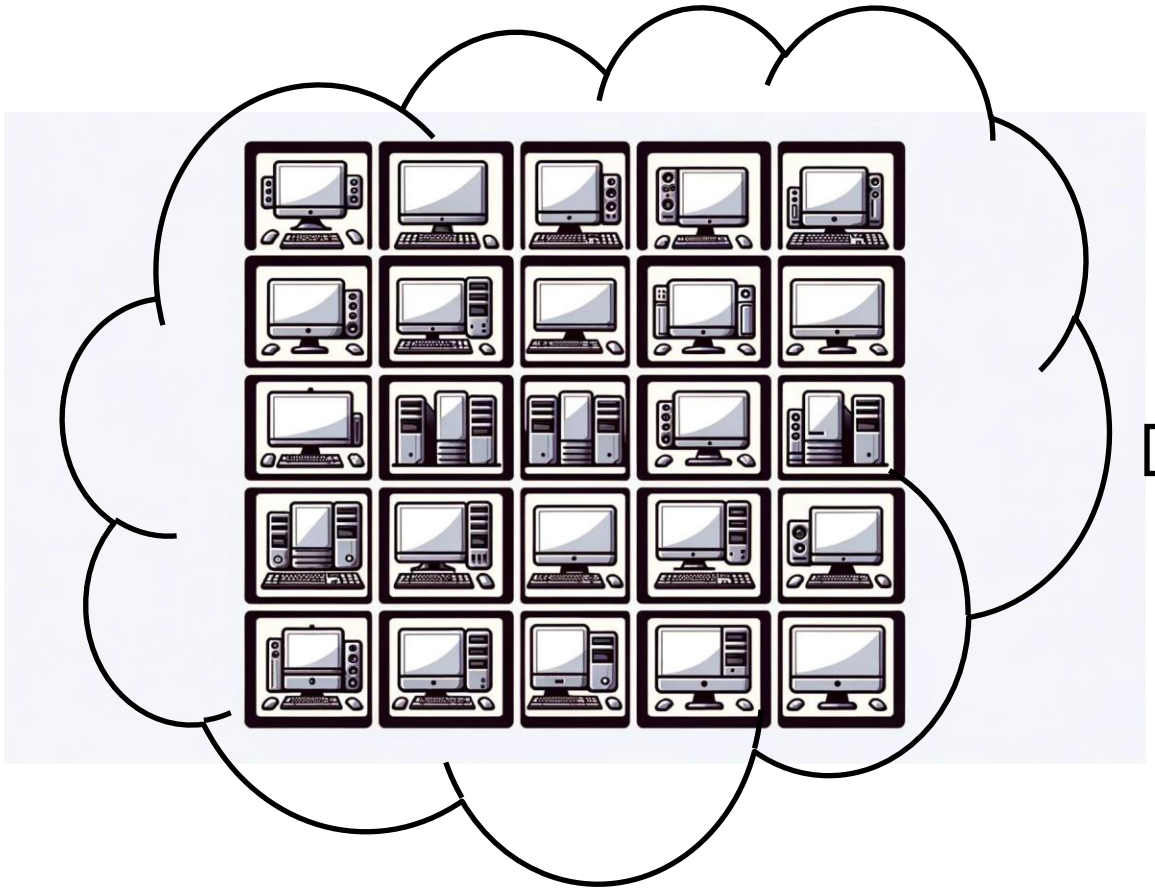
- like an operating system, a blockchain protocol:
  - acts as a “master program” to coordinate all apps/smart contracts
  - provides a virtual machine to developers of applications
- like the Internet, the product of collaboration between many physical machines

A “Decentralized” Virtual Machine



network of physical computers

A “Decentralized” Virtual Machine



network of physical computers
+ blockchain protocol

simulated (virtual) computer

High-Level Syllabus

This course: building the “computer in the sky.”

High-Level Syllabus

This course: building the “computer in the sky.”

Part I: low-performance, “permissioned” blockchain protocols.

- fault-tolerant consensus, virtual machine execution

High-Level Syllabus

This course: building the “computer in the sky.”

Part I: low-performance, “permissioned” blockchain protocols.

- fault-tolerant consensus, virtual machine execution

Part II: performance and scaling.

- Merkle trees, rollups (optimistic and “zk”) and sequencers, SNARKs, light clients, bridges, data availability, transaction fee mechanisms, etc.

High-Level Syllabus

This course: building the “computer in the sky.”

Part I: low-performance, “permissioned” blockchain protocols.

- fault-tolerant consensus, virtual machine execution

Part II: performance and scaling.

- Merkle trees, rollups (optimistic and “zk”) and sequencers, SNARKs, light clients, bridges, data availability, transaction fee mechanisms, etc.

Part III: permissionless protocols.

- proof-of-work vs. proof-of-stake, incentives, public mempools, MEV, etc.

Comments

1. Course is about a new computing paradigm, not digital money.
   - blockchains ≠ cryptocurrencies
   - a general-purpose technology

Comments

1. Course is about a new computing paradigm, not digital money.
   - blockchains ≠ cryptocurrencies
   - a general-purpose technology
2. Principles over protocols.
   - though will learn a lot about Ethereum, Bitcoin, etc. along the way

Comments

1. Course is about a new computing paradigm, not digital money.
   - blockchains ≠ cryptocurrencies
   - a general-purpose technology
2. Principles over protocols.
   - though will learn a lot about Ethereum, Bitcoin, etc. along the way
3. A new area of computer science.
   - and you can get in on the ground floor! (like Internet/Web in 1990s)
   - course is a one-stop shop to prepare for industry or research

Deliverables

1. Team research project (50%).
   - team size 3-4, project proposal due in mid-March
   - can be pure theory, pure implementation, anywhere in between

Deliverables

1. Team research project (50%).
   - team size 3-4, project proposal due in mid-March
   - can be pure theory, pure implementation, anywhere in between
2. Homeworks (40%).
   - around 8-9 over course of semester, can work in pairs
   - mix of going deeper on lecture material, reading responses, interacting with the broader Web 3 ecosystem

Deliverables

1. Team research project (50%).
   - team size 3-4, project proposal due in mid-March
   - can be pure theory, pure implementation, anywhere in between
2. Homeworks (40%).
   - around 8-9 over course of semester, can work in pairs
   - mix of going deeper on lecture material, reading responses, interacting with the broader Web 3 ecosystem
3. Participation (10%).
   - showing up to lecture, participation in lecture/forum, etc.
   - we reserve the right to give occasional pop quizzes in class

Course Staff

Instructor: Tim Roughgarden

- office hours after class (until 10:45am)

TA: Naveen Durvasula

- office hours TBA

TA: Yuval Efron

- office hours Tuesday 10am-noon

URL: https://timroughgarden.org/s25/