Blockchain Principles and Applications

Amir Mahdi Sadeghzadeh, PhD

Data and Network Security Lab (DNSL)
Trustworthy and Secure AI Lab (TSAIL)

Most slides have been adapted from ECE/COS 470, Pramod Viswanath, Princeton 2024 and CS251, Dan Boneh, Stanford 2023.

Course information

- Course Number: 40875-1
  - Time: Sun. - Tues. 10:30 – 12:00
  - Rooms: CE-201 and https://vc.sharif.edu/ch/amsadeghzadeh

- Instructor
  - Amir Mahdi Sadeghzadeh (amsadeghzadeh@gmail.com)
  - Office: CE-704
  - Lab: CE-502
  - Office hours: by appointment and through email

Course information

- Course website: **sharif-blockchain.github.io**
  - Syllabus, Lecture slides, Assignments, etc

- Quera: Quera page https://quera.org/course/add_to_course/course/20720/
  - Discussions and HWs

- Tas
  - Amir Mohammad Aghapour
  - Erfan Bahrami

Refrences

- Lecture slides and supplementary reading material

- Bitcoin and Cryptocurrency Technologies, A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, Princeton University Press. Henceforth termed as PUP (Princeton university press).

- Introduction to Cryptocurrencies, a basic online course by Haseeb Qureshi.

- ECE/COS 470: Principles of Blockchains, Princeton University, Professor: Pramod Viswanath, Lecture Nots

Prerequisites

- The basic technical prerequisites are a background in probability and algorithms. Decent amount of software programming background is essential.

Grading Policy

- Assignments (30%)
- Midterm (and Mini-Exam) (20%)
- Final (30%).
- Paper review and presentation (20%)

Assignments

- There are 3 or 4 Assignments
- Late policy
  - All students have 7 free late days for the assignments
  - You can distribute them as you want across your HWs
  - No more than 3 days for each homework
  - All subsequent late submissions will accrue a 20% penalty
- Ethics statement
  - Please read Sharif CE Department Ethics Statement
  - Every student must solve every homework by themselves
    - You may discuss the assignments with your friends, but when you finally solve it, every line of your code (except libraries that have been okayed by course staff) must be written by you
    - Your solution must be yours

Presentations

- Each persons has two presentations
- Should cover (at least) one paper or blog assigned for reading
- The list of candidate papers is determined by the instructor.
- Allocate enough time to make the presentation, it is not as easy as you think
- Will be evaluated by the instructor, TAs, and your classmates

Presentation rubric

- Technical
  - Depth of content
  - Accuracy of content
  - Paper criticism
  - Discussion lead

- Soft presentation skills
  - Time management
  - Responsiveness to audience
  - Organization
  - Presentation aids

Course Outline

- Reviewing cryptographic primitives
- Foundations of Blockchain
  - Nakamoto consensus, P2P networks, Bitcoin system, Bitcoin safety and liveness.
- Scaling Solutions
  - Layer 1 (on-chain) & Layer 2 (off-chain) techniques, sharding, and rollups.
- Beyond Bitcoin
  - Ethereum, Decentralized Apps, EVM, Smart contracts.
- Privacy on a public blockchain
  - Zero-knowledge proofs, anonymous transactions, and regulatory challenges.

☺

Welcome to the Blockchain Principles & Applications Course!

What are Blockchains?

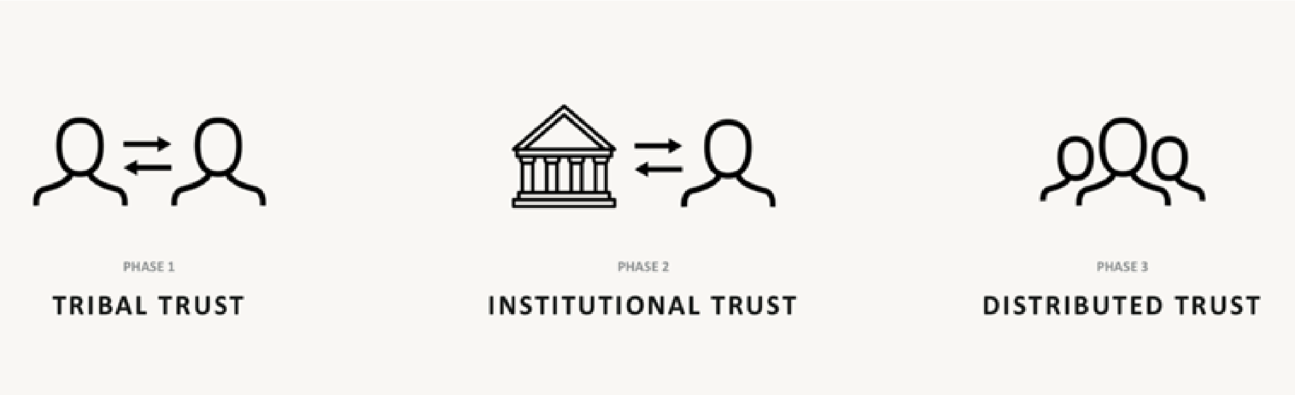
Blockchains are decentralized digital trust platforms

Decentralized system

- No single entity (person/company) is responsible for the smooth operation of the system.
    - Blockchains are peer-to-peer systems
        - each peer has the same prescribed behavior
        - No peer is unique.
        - Peers communicate with each other by exchanging messages
        - Beyond this message exchange, peers function independently of one another.

Trust

- Human success is based on flexible cooperation in large numbers. This requires trust!



Evolution of Trust over human history

Platform Economy

2023 September
Top US companies by market cap

1.	Apple	$2.9 T
2.	Microsoft	$2.5 T
3.	Alphabet	$1.7 T
4.	Amazon	$1.4 T
5.	Nvidia	$1.2T
6.	Tesla	$0.8 T

2011
Top US companies by market cap

1.	Exxon	$417 B
2.	Apple	$321 B
3.	Chevron	$215 B
4.	Microsoft	$213 B
5.	IBM	$207 B
6.	Walmart	$204 B

A Decentralized Platform?

- A decentralized Dropbox, eBay, Instagram?
- Incentives aligned with consumers and resource providers?
- No need for a trusted middle party?

Such is the siren song of blockchains

Bitcoin: the original blockchain

Cryptocurrency

medium of exchange and store of value

Born during the **2008 Financial Crisis**

Anonymous inventor

pseudonym: Satoshi Nakamoto

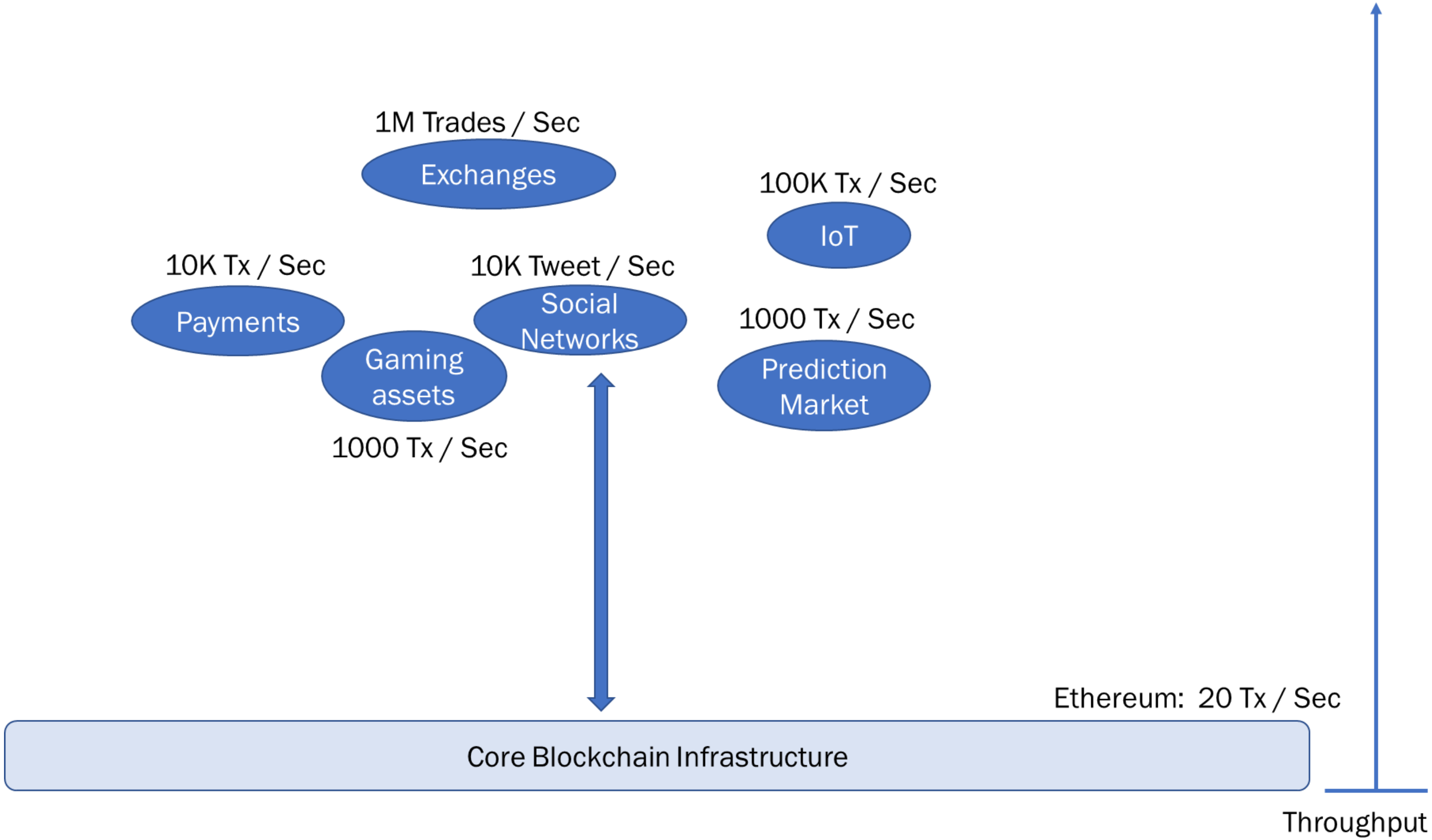
Very secure

no attacks, has been live continuously

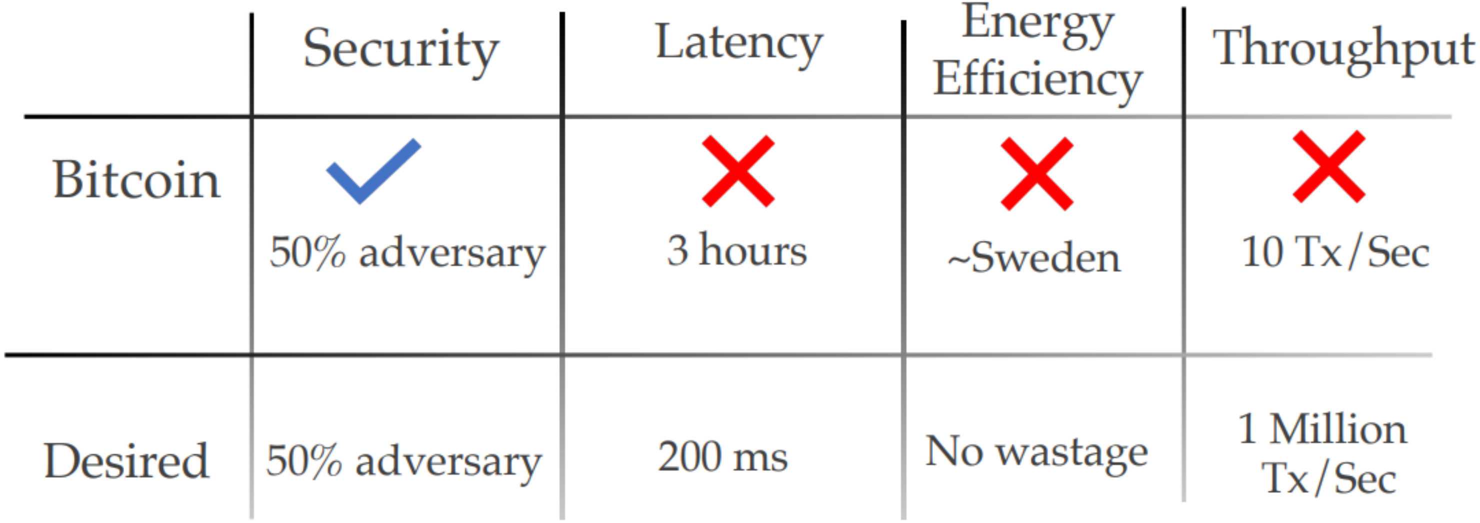
Bitcoin performance

1. Security	– 50% adversary
2. Transaction throughput	– 7 tx/s
3. Confirmation Latency	– hours
4. Energy consumption	– medium size country
5. Compute	– specialized mining hardware
6. Storage	– everyone stores everything
7. Communication	– everyone tx/rx everything

Bitcoin is far from a Platform



Blockchain Today



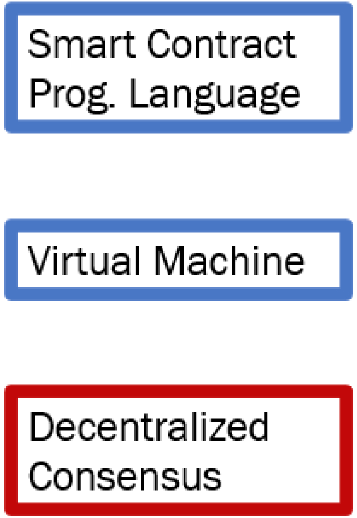
	Security	Latency	Energy Efficiency	Throughput
Bitcoin	✓ 50% adversary	✗ 3 hours	✗ ~Sweden	✗ 10 Tx/Sec
Desired	50% adversary	200 ms	No wastage	1 Million Tx/Sec

Building Block of Blockchains

- Platforms are applications built on networked computers
- Basic building block: Decentralized Computer
  - Multiple untrusted computers interacting with one another, forming consensus on an ordered list of instructions
  - A virtual machine interprets the instruction set
  - A programming language and a corresponding compiler provide a forum for decentralized applications (dApps)

Technical Components

- Decentralized Computer
  - Cryptographic data structures
  - Disk I/O and Database management
  - Memory management
  - Operating systems
  - Peer to peer networking
  - Consensus and distributed algorithms
- Virtual Machine
  - Reduced instruction set, incentives
  - General purpose programming language



Smart Contract Prog. Language

Virtual Machine

Decentralized Consensus

Nearly all aspects of Computer Science

Technical Challenges

- **Permissionless**
  - Anyone can meaningfully participate
  - **Challenge**: need to prevent spam, bad actors

- **Dynamic availability and safety**
  - Consensus holds with dynamic participation of enough participants
  - **Challenge**: need to work even with bad actors

- **Cryptography**
  - Provides basic tools to address both design goals
  - **Challenge**: "The trouble is, the other side can do magic too, Prime Minister."

Principles of Blockchains

- **Conceptual** Principles
  - Algorithmic designs
  - Byzantine resistance
  - Security analysis
  - Mechanism design and incentive compatibility

- **Engineering** Principles
  - Modular software stack
  - Software engineering
  - Integration and composition of different modules – secure, yet efficient

What is a blockchain for?

Abstract answer: a blockchain provides
coordination between many parties,
when there is no single trusted party

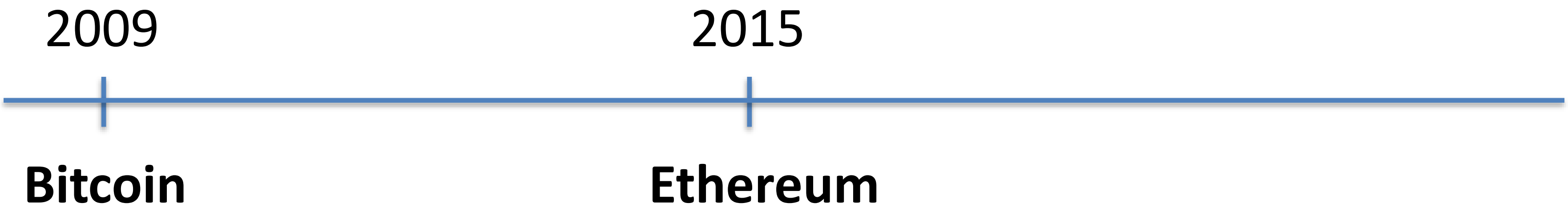
if trusted party exists ⇒ no need for a blockchain

Blockchains: what is the new idea?

Several innovations:

- A practical **public append-only data structure**, secured by replication and incentives
- A fixed supply asset (BTC). Digital payments, and more.

Blockchains: what is the new idea?



2009

2015

Bitcoin

Ethereum

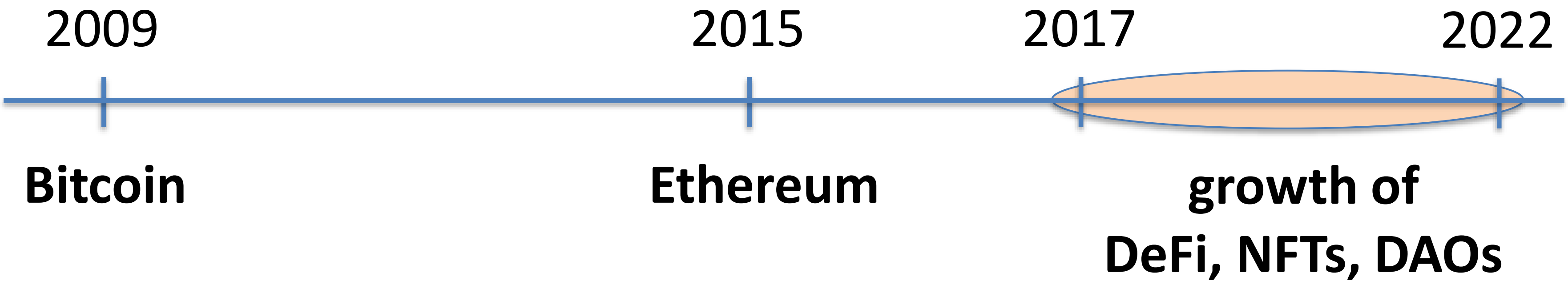
Several innovations:

- **Blockchain computer**: a fully programmable environment

  ⟹ public programs that manage digital and financial assets

- **Composability**: applications running on chain can call each other

Blockchains: what is the new idea?



2009

2015

2017

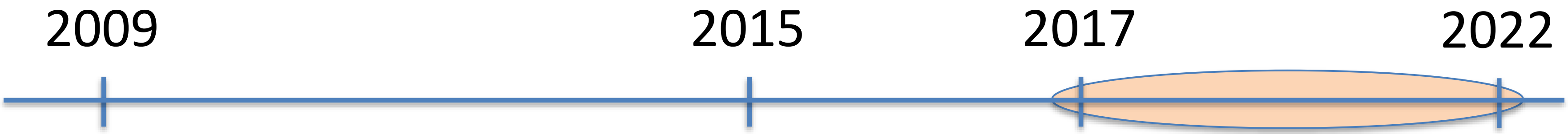
2022

Bitcoin

Ethereum

growth of
DeFi, NFTs, DAOs

Blockchains: what is the new idea?



2009 2015 2017 2022

Bitcoin

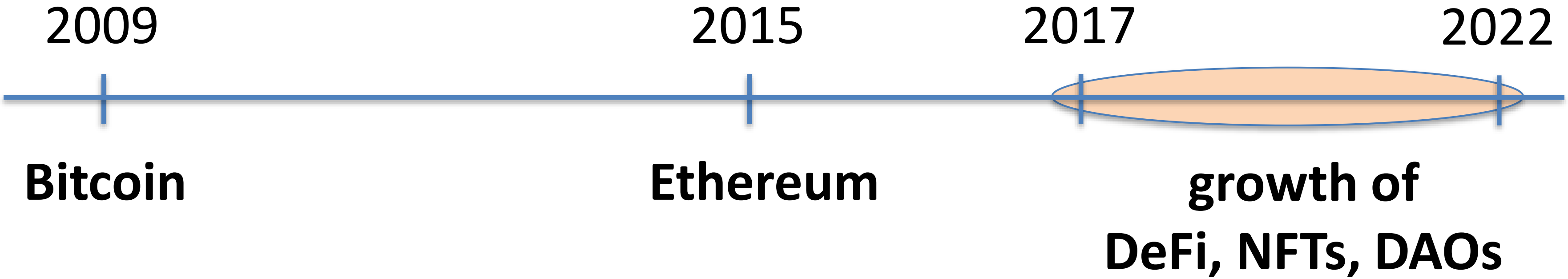
Ethereum

growth of
DeFi, NFTs, DAOs

DeFi (Decentralized Finance)

- Built on blockchain technology, primarily Ethereum
  - operate without intermediaries like banks.
    - It includes lending, borrowing, trading, and earning interest on crypto assets.

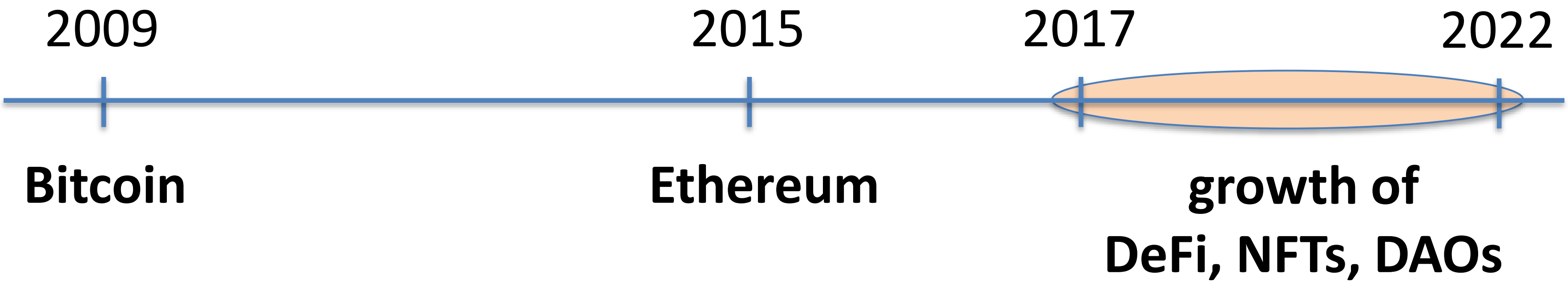
Blockchains: what is the new idea?



NFTs (Non-Fungible Tokens)

- Unique digital assets that represent ownership of items like art, music, collectibles, and even virtual real estate.

Blockchains: what is the new idea?



2009 **Bitcoin**

2015 **Ethereum**

2017 – 2022 **growth of DeFi, NFTs, DAOs**

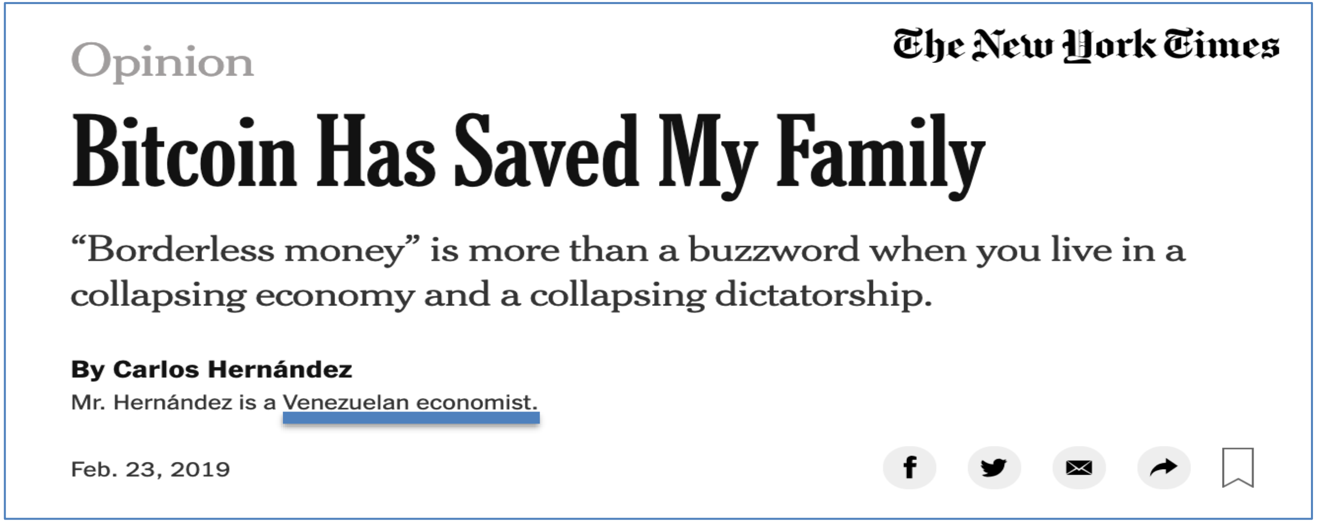
DAOs (Decentralized Autonomous Organizations)

- DAOs are organizations governed by smart contracts and community voting, rather than centralized leadership.

So what is this good for?

(1) Basic application: a digital currency (stored value)

- Current largest: Bitcoin (2009),   Ethereum (2015)
- Global: accessible to anyone with an Internet connection



Opinion

The New York Times

Bitcoin Has Saved My Family

“Borderless money” is more than a buzzword when you live in a collapsing economy and a collapsing dictatorship.

By Carlos Hernández

Mr. Hernández is a Venezuelan economist.

Feb. 23, 2019

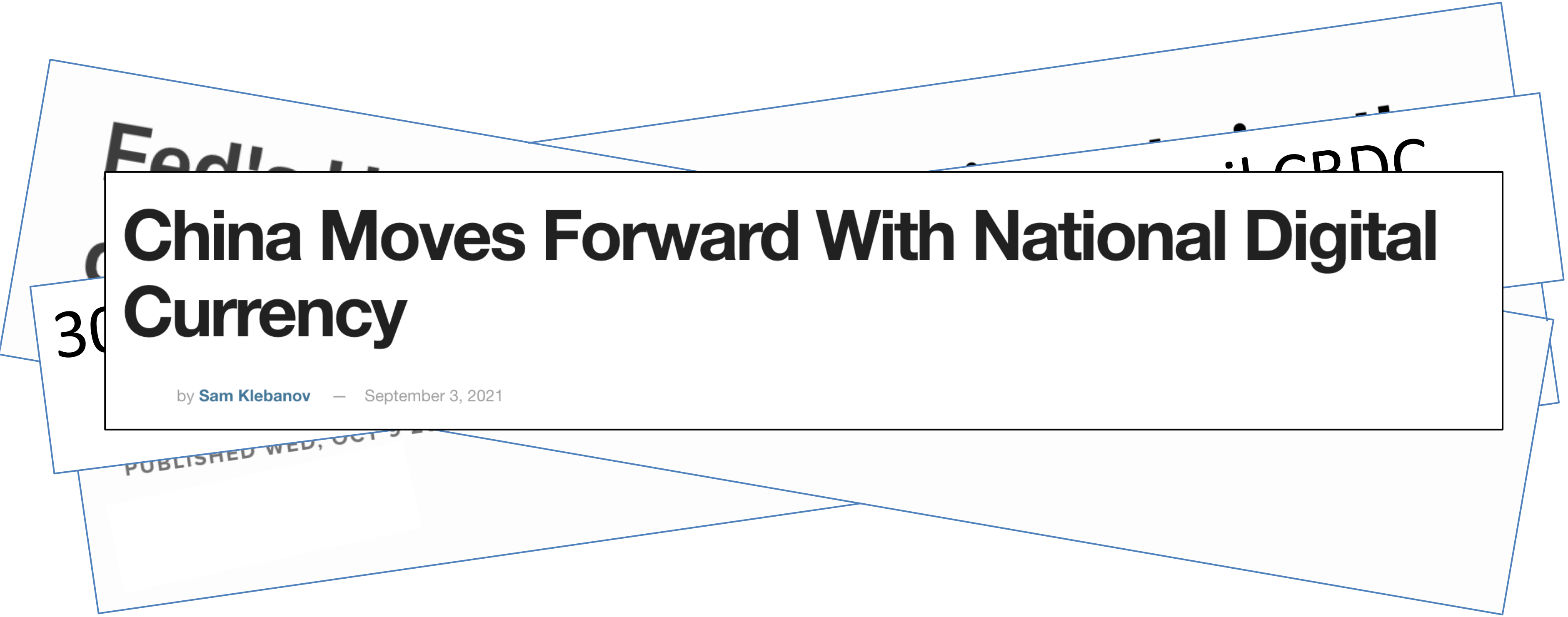
What else is it good for?

(2) Decentralized applications (DAPPs)

- **DeFi**: financial instruments managed by public programs
  - examples: stablecoins, lending, exchanges, ….
- **Asset management** (NFTs)**:** art, game assets, domain names.
- **Decentralized organizations** (DAOs): (decentralized governance)
  - DAOs for investment, for donations, for collecting art, etc.

(3) New programming model: writing decentralized programs

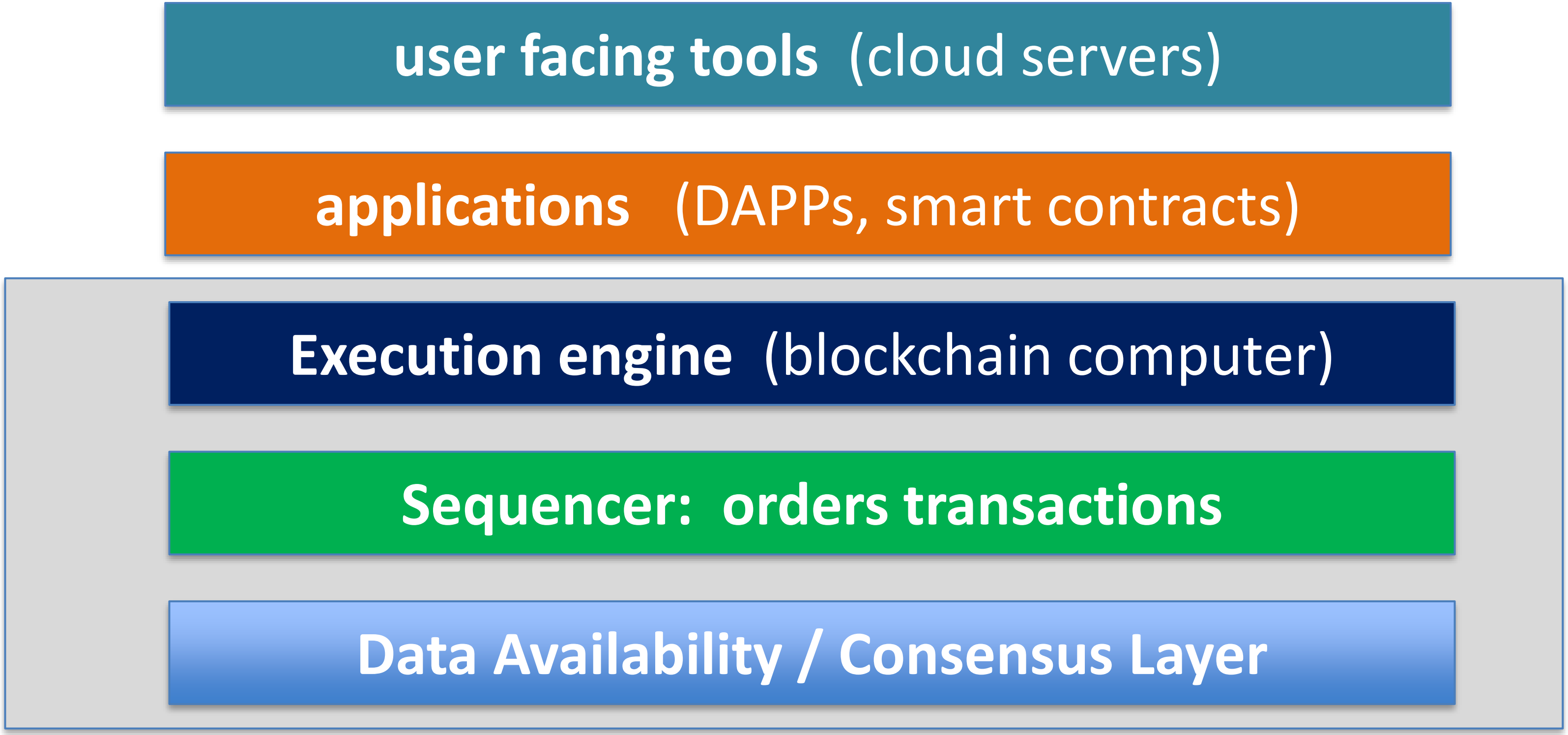
Central Bank Digital Currency (CBDC)



China Moves Forward With National Digital Currency

by Sam Klebanov — September 3, 2021

What is a blockchain?



user facing tools (cloud servers)

applications (DAPPs, smart contracts)

Execution engine (blockchain computer)

Sequencer: orders transactions

Data Availability / Consensus Layer

Consensus layer (informal)

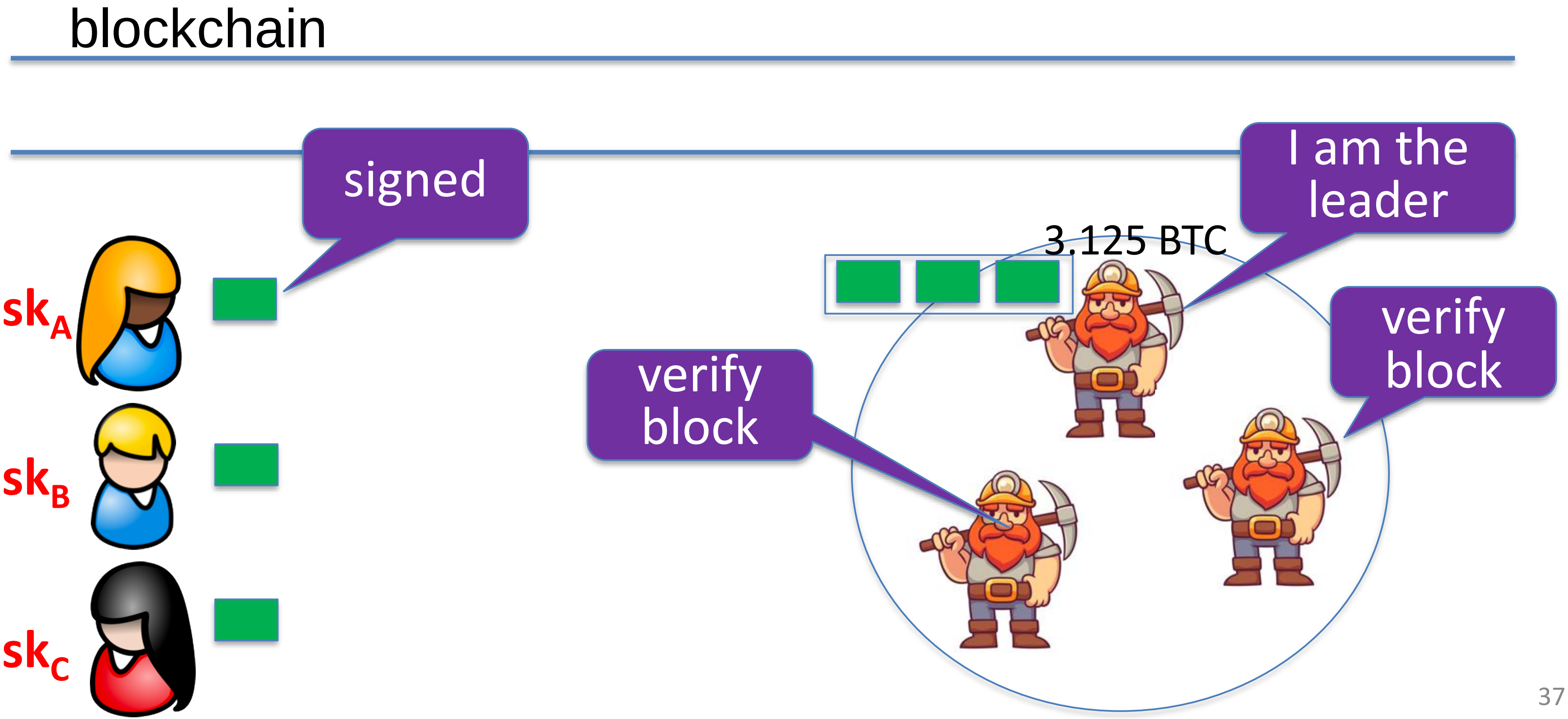
achieved by replication

A **public** append-only data structure:

- **Persistence**: once added, data can never be removed*
- **Safety**: all honest participants have the same data**
- **Liveness:** honest participants can add new transactions
- **Open(?)**: anyone can add data (no authentication)

Data Availability / Consensus layer

How are blocks added to chain?



blockchain

signed

sk_A

sk_B

sk_C

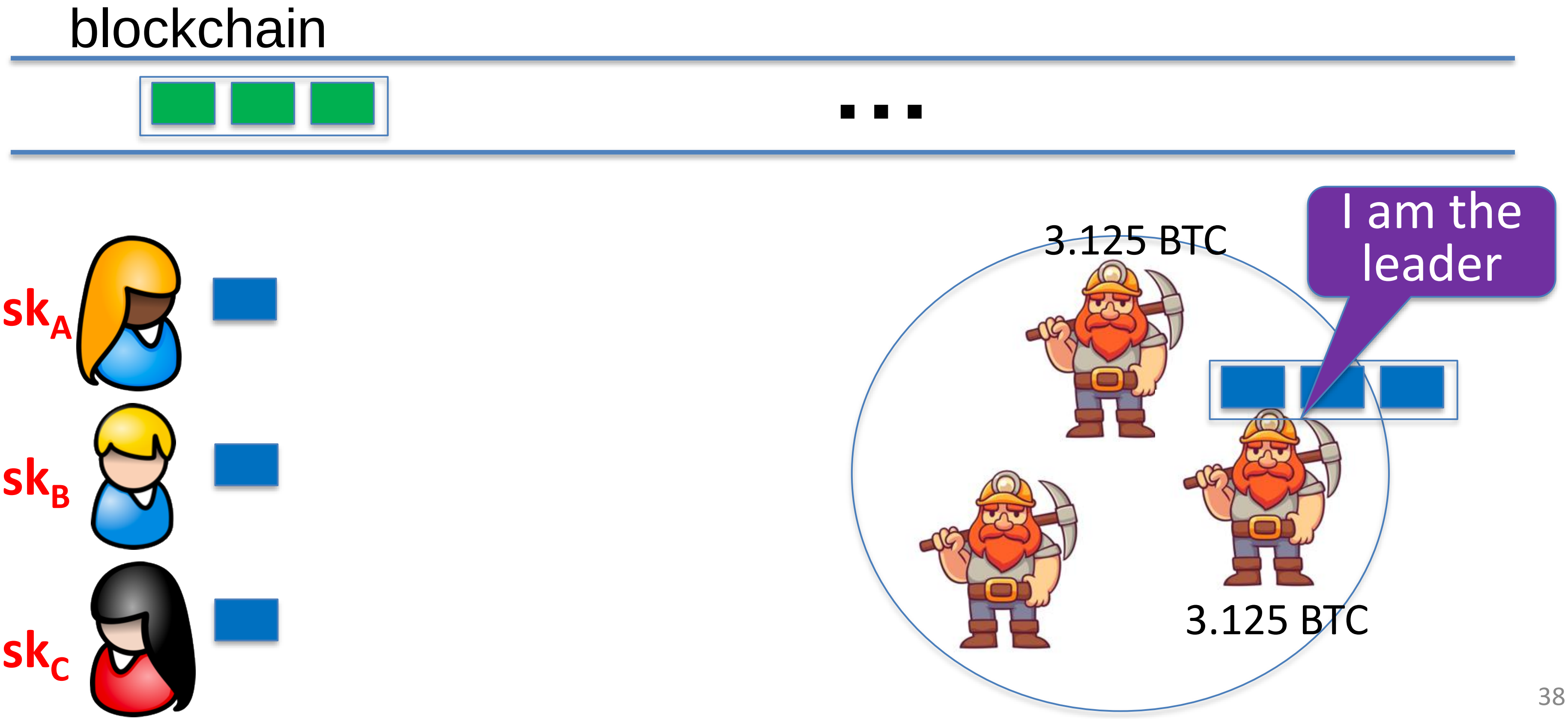
verify block

3.125 BTC

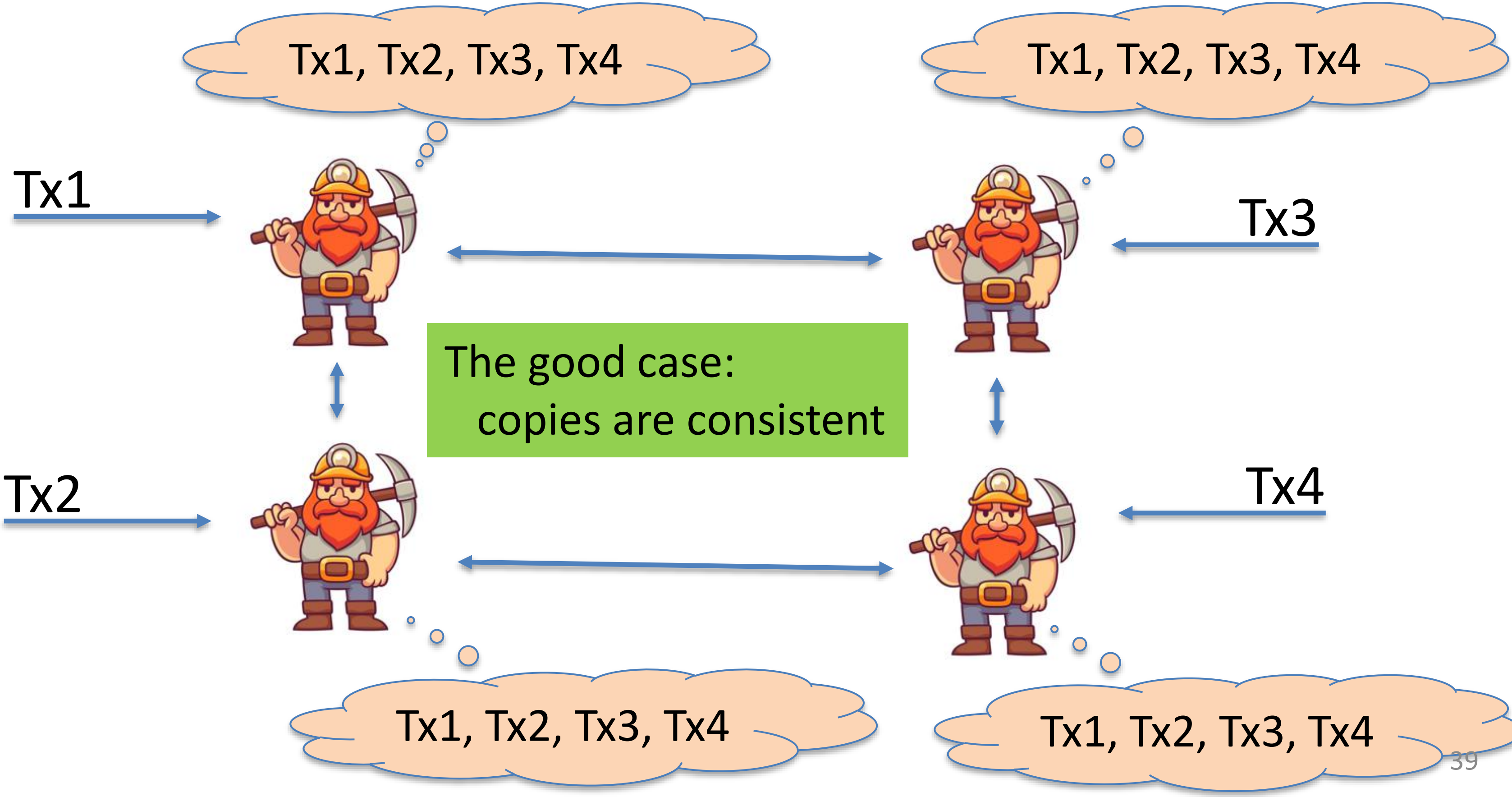
I am the leader

verify block

How are blocks added to chain?



Why is consensus a hard problem?

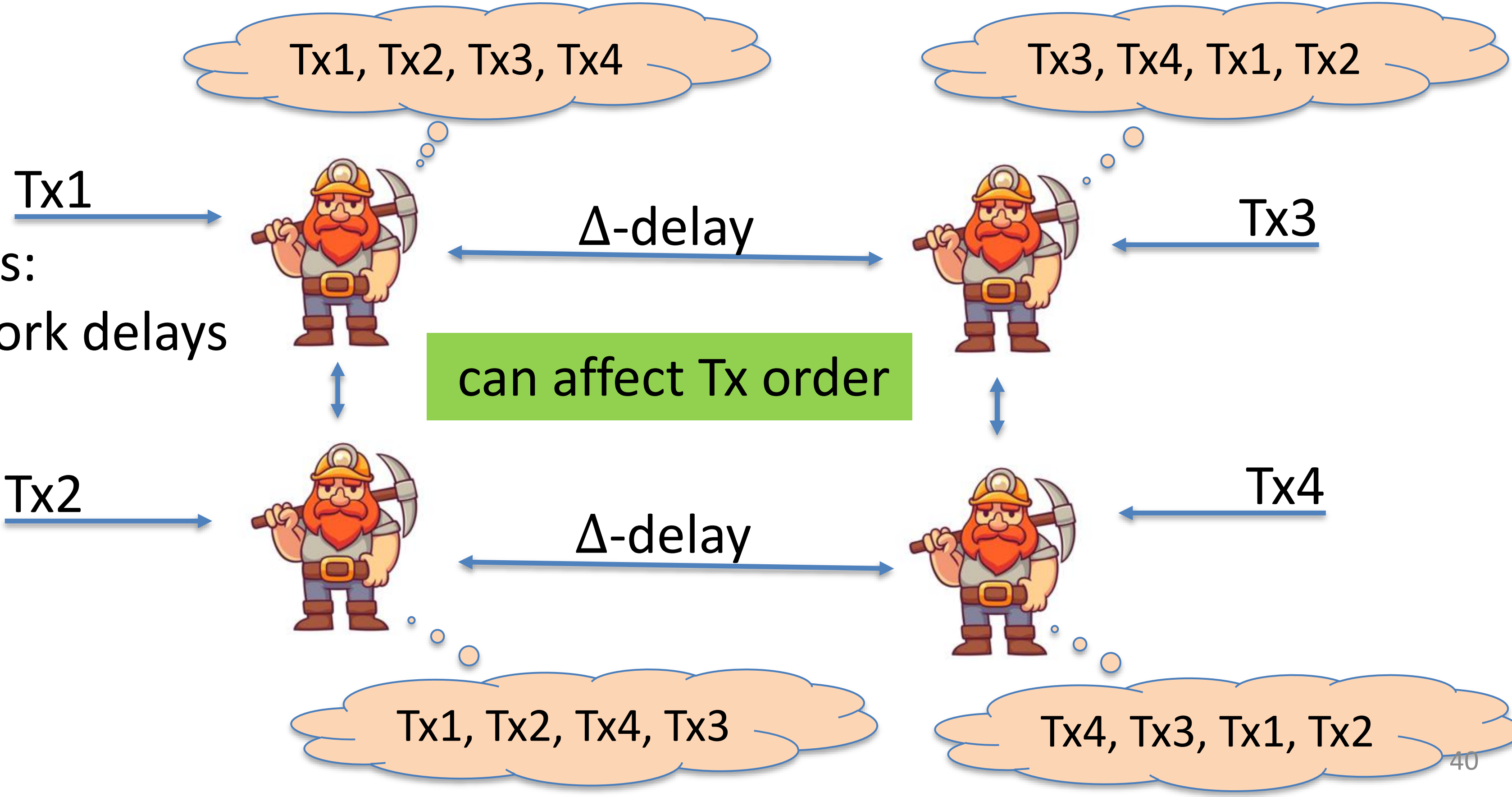


The good case:
copies are consistent

Why is consensus a hard problem?

Problems:

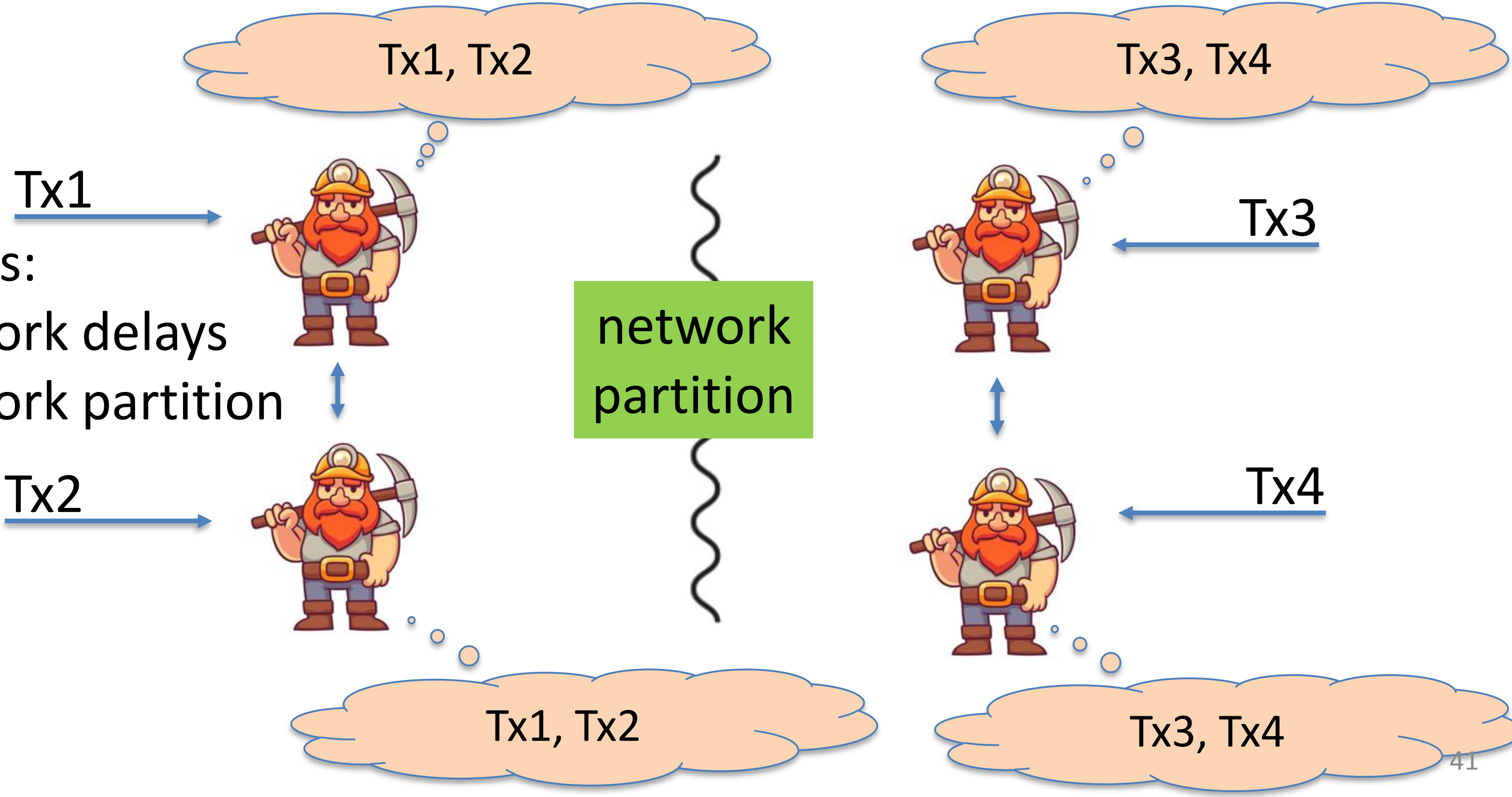
- Network delays



Why is consensus a hard problem?

Problems:

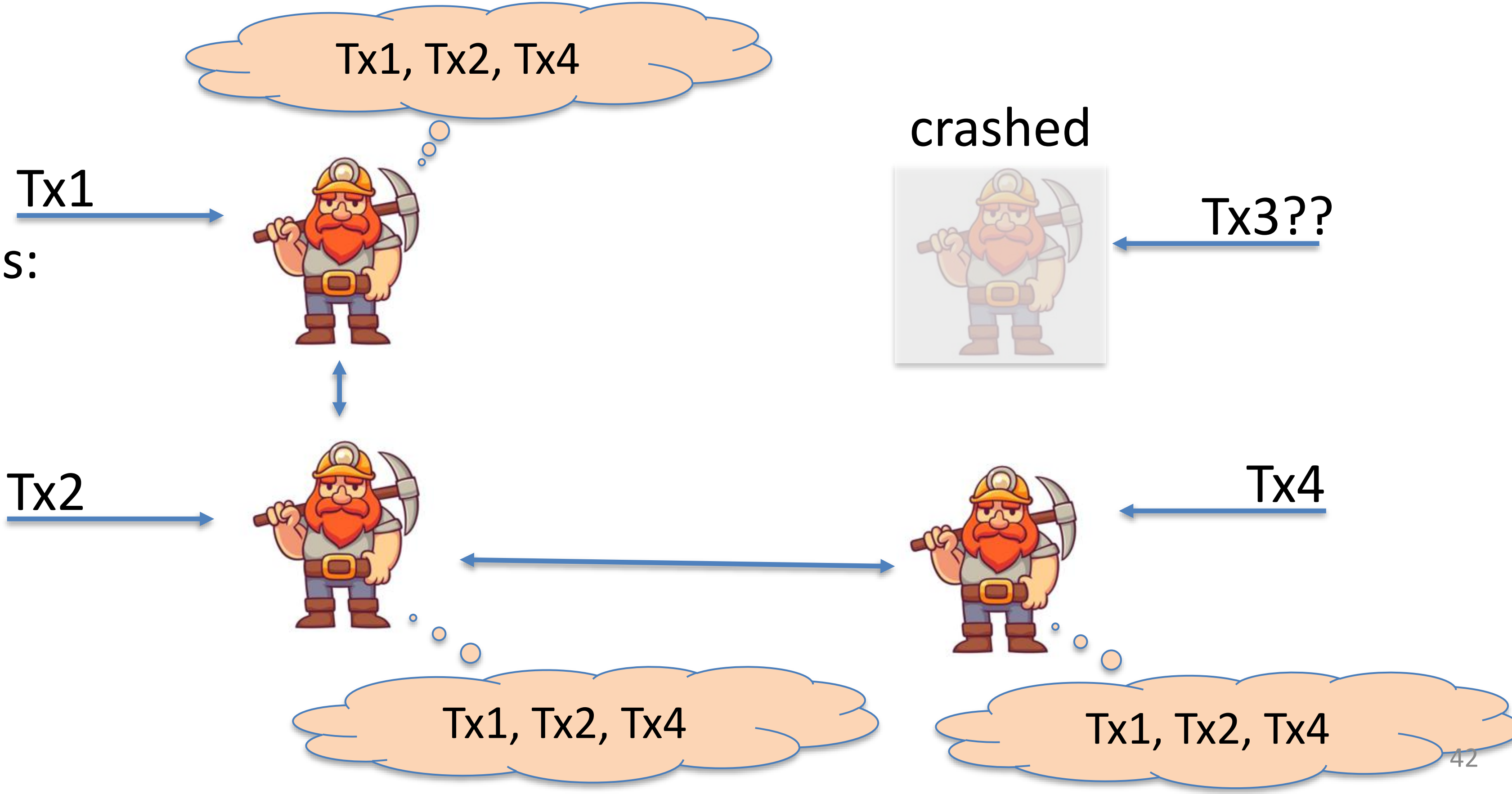
- Network delays
- Network partition



Why is consensus a hard problem?

Problems:

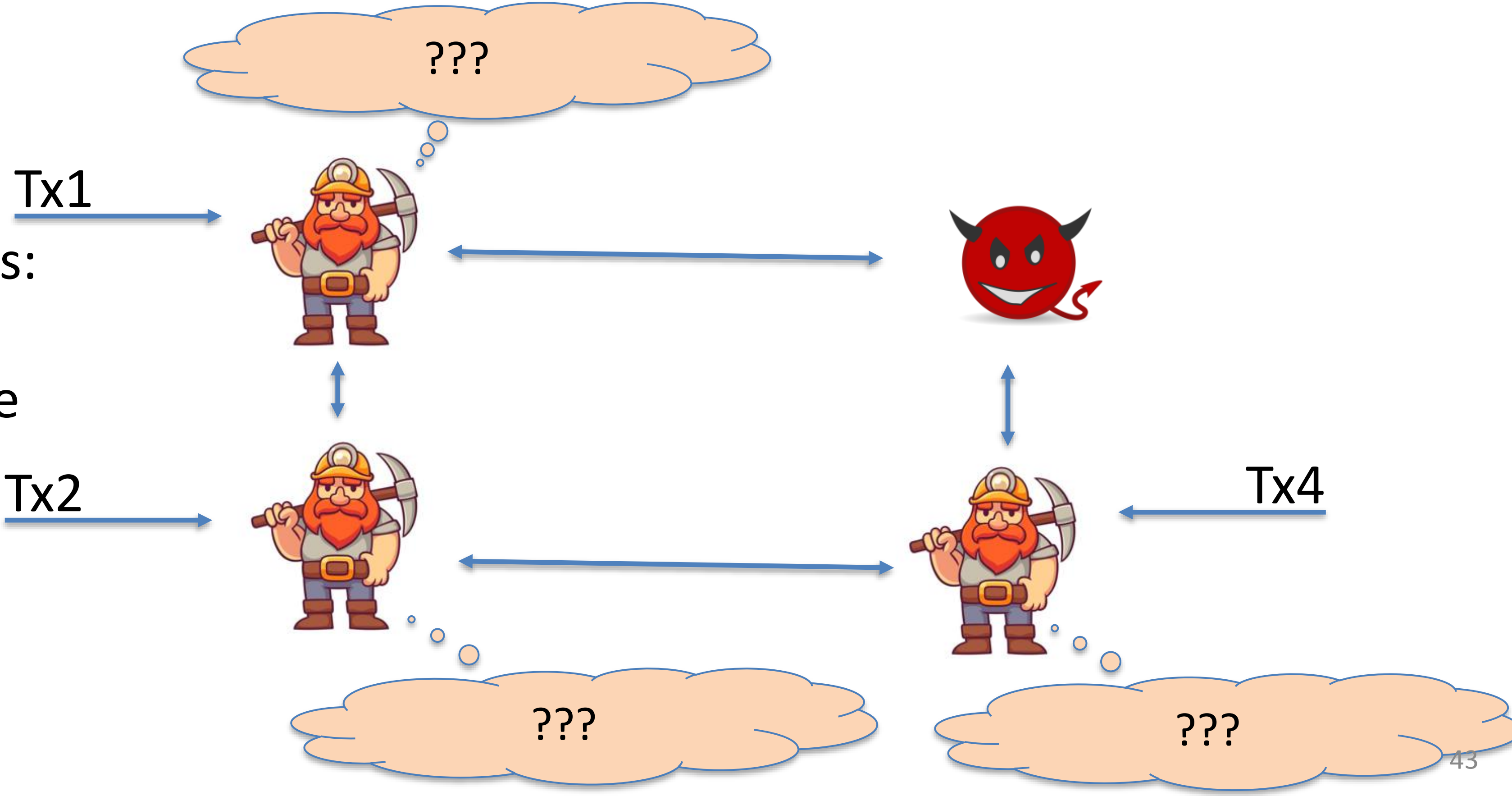
- crash



Why is consensus a hard problem?

Problems:

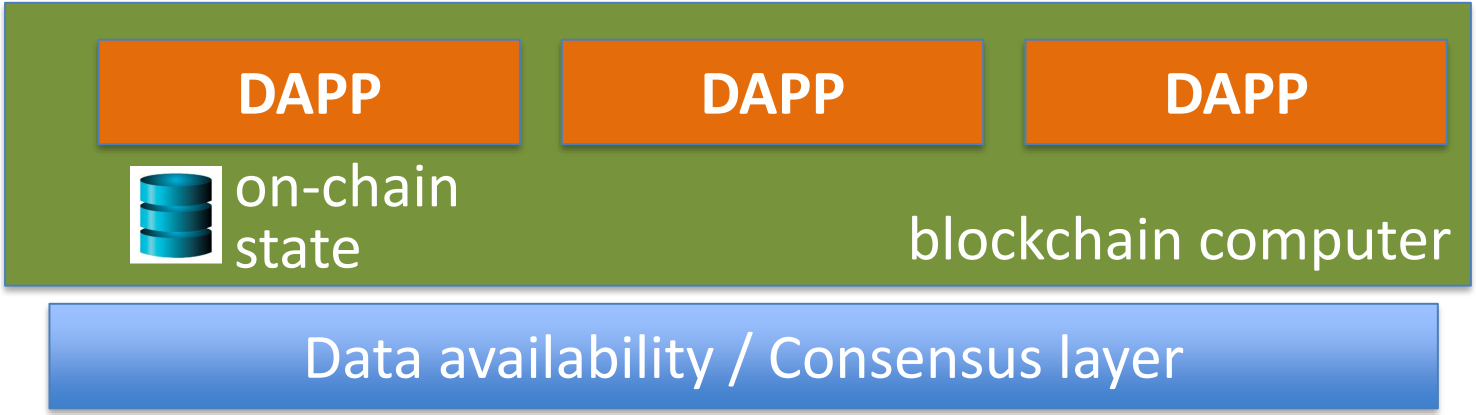
- crash
- malice



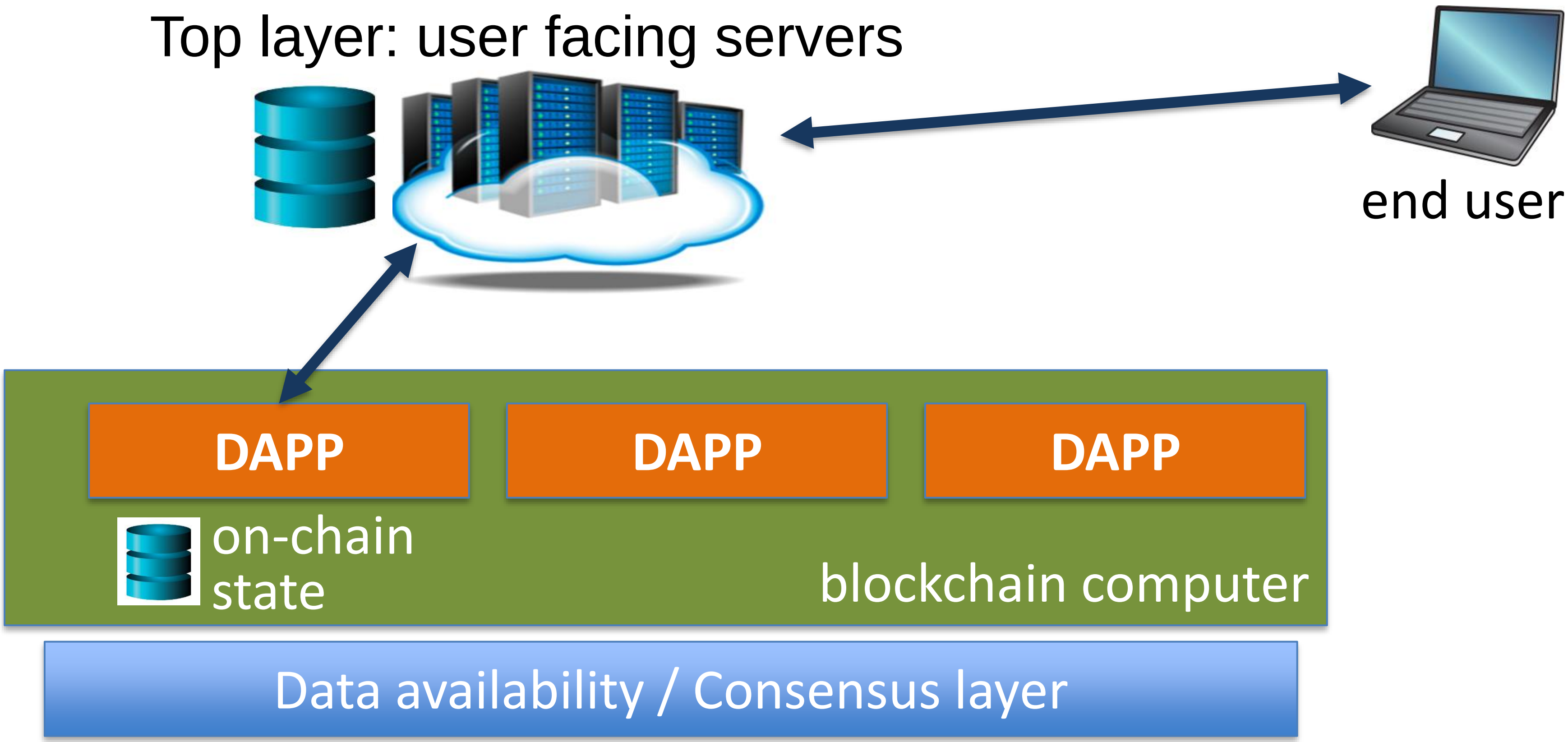
Next layer: the blockchain computer

Decentralized applications (DAPPs):

- Run on blockchain: code and state are written on chain
- Accept Tx from users ⇒ state transitions are recorded on chain



Next layer: the blockchain computer



Top layer: user facing servers

end user

DAPP

DAPP

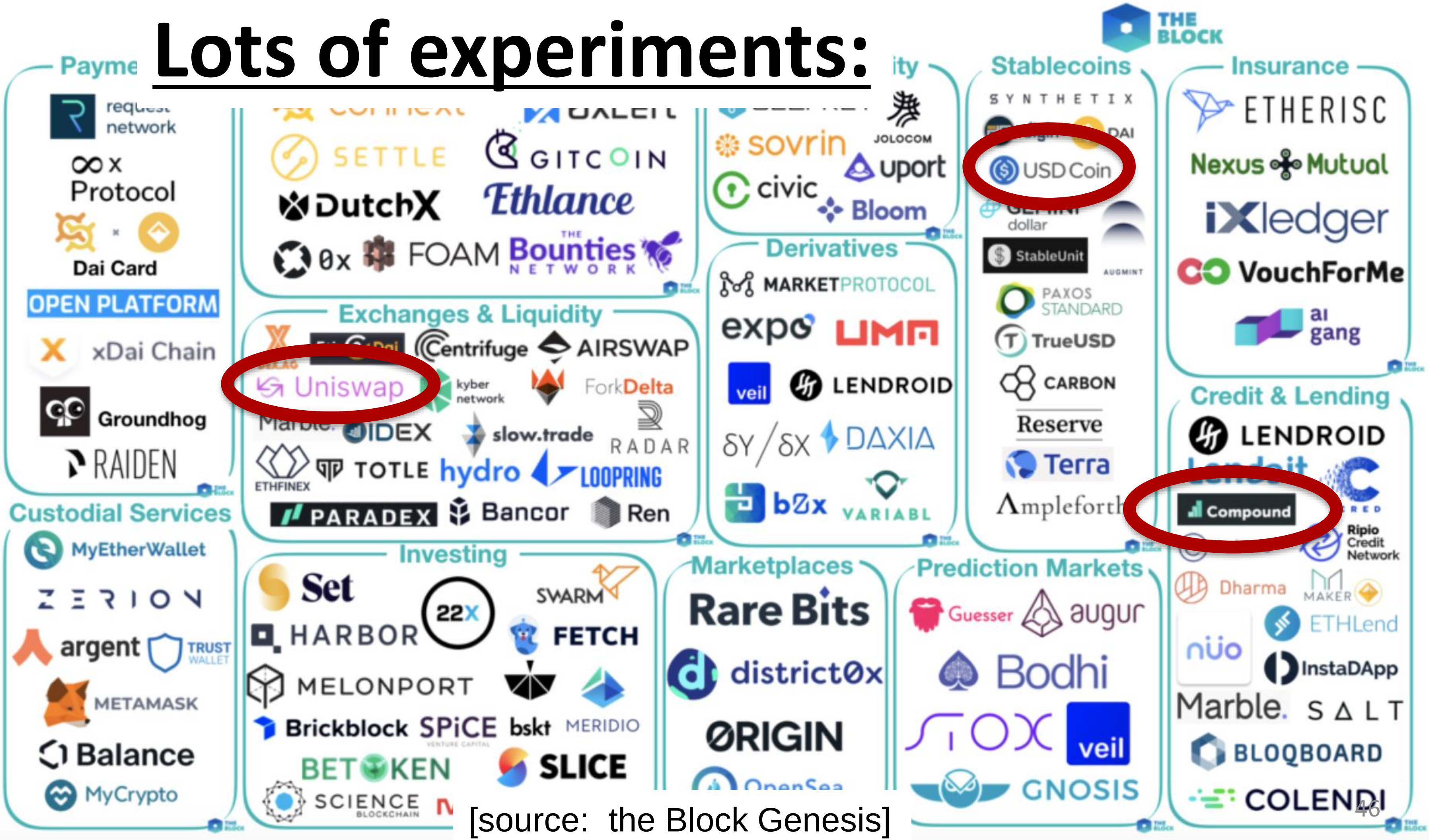
DAPP

on-chain state

blockchain computer

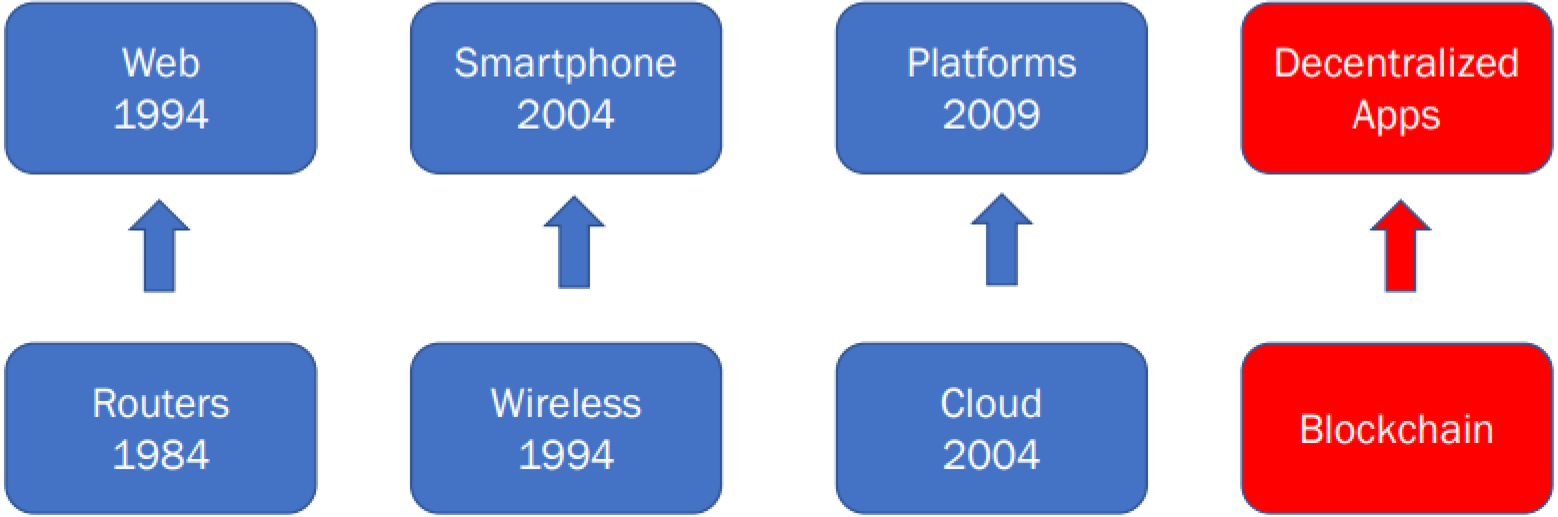
Data availability / Consensus layer

Lots of experiments:



[source: the Block Genesis]

Infrastructure to applications



Web
1994

Routers
1984

Smartphone
2004

Wireless
1994

Platforms
2009

Cloud
2004

Decentralized
Apps

Blockchain

Resources

- ECE/COS 470, Pramod Viswanath, Princeton 2024
- CS251, Dan Boneh, Stanford 2023