Engineering Blockchain and Web3 Apps

Ronghui Gu

Fall 2024

Columbia University

Course website: https://verigu.github.io/6998Fall2024/

Instructor

Prof. Ronghui Gu

515 Computer Science Building

ronghui.gu@columbia.edu

Office hours: Wed, 1-2pm EST by zoom

Research: formal verification and software security

Startup: 

1 Bite Size Blockchain

Blockchain and Bitcoin

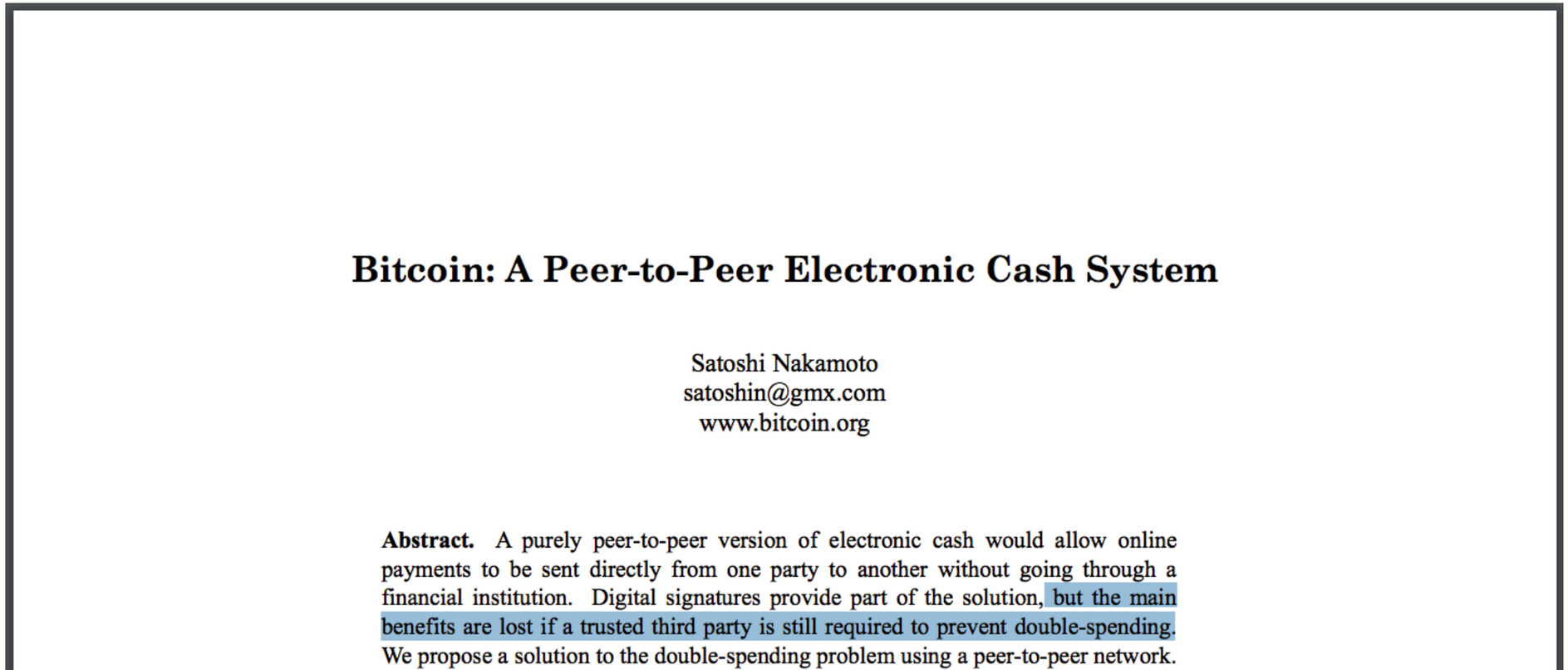
Bitcoin ≠ Blockchain

Fuel and products of the Bitcoin blockchain

A decentralized system

Blockchain and Bitcoin

- Electronic cash system
- Peer-to-peer
- A decentralized ledger (a trusted third party should be removed)



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

A Centralized Electronic Cash System …

Centralized Ledger

Bank
Paypal
…

Alice —> Bob $10
Bob —> Alice $5

Limitations

Trust the 3rd party
Opaque system
Mutable
…

Alice $20, Bob $10 ⟶ Alice $15, Bob $15

Blockchain (informal)

Decentralized Ledger

Peer-to-peer

...

Alice —> Bob $10
Bob —> Alice $5

Goals

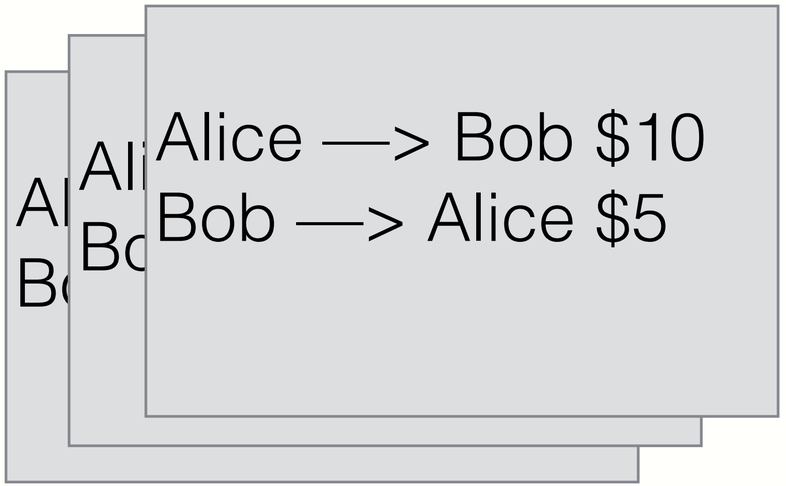
No trusted 3rd party
Transparent system
Immutable

...

Alice $20, Bob $10 ⟶ Alice $15, Bob $15

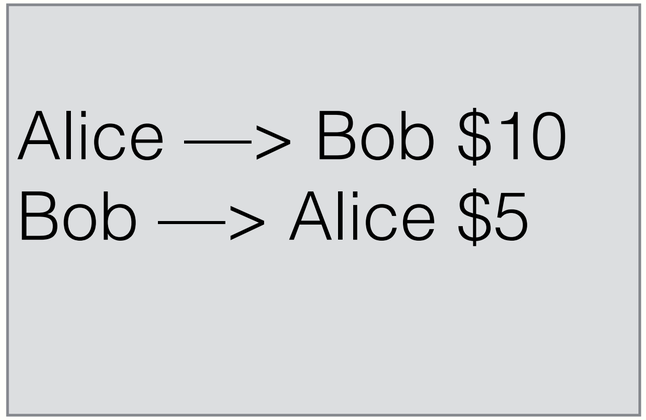
Blockchain (informal)

A Blockchain is a Decentralized Ledger



Blockchain (informal)

A block is one page of the Decentralized Ledger



Blockchain (informal)

The question is who has the bookkeeping right?

Alice —> Bob $10
Bob —> Alice $5

Consensus protocol

- Random?
- One person, one vote?
- Based on stake?

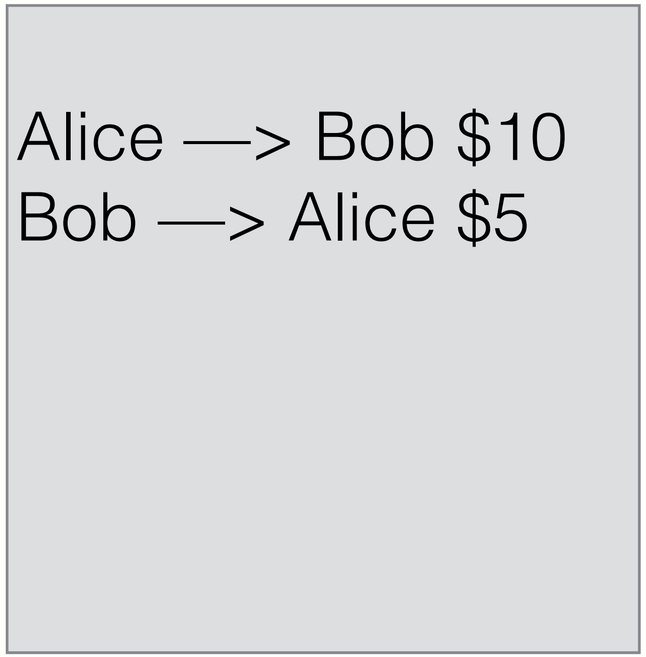
Blockchain (informal)

One person, one vote

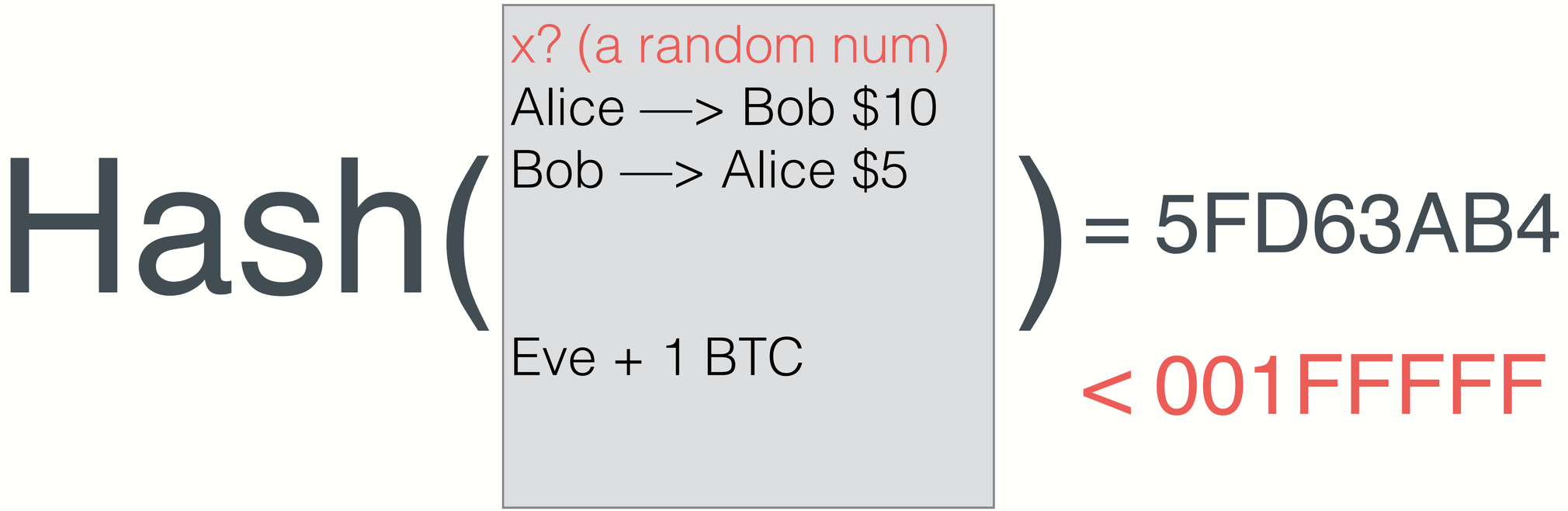
One CPU, one vote

- Computation power

Bitcoin Ming (informal)

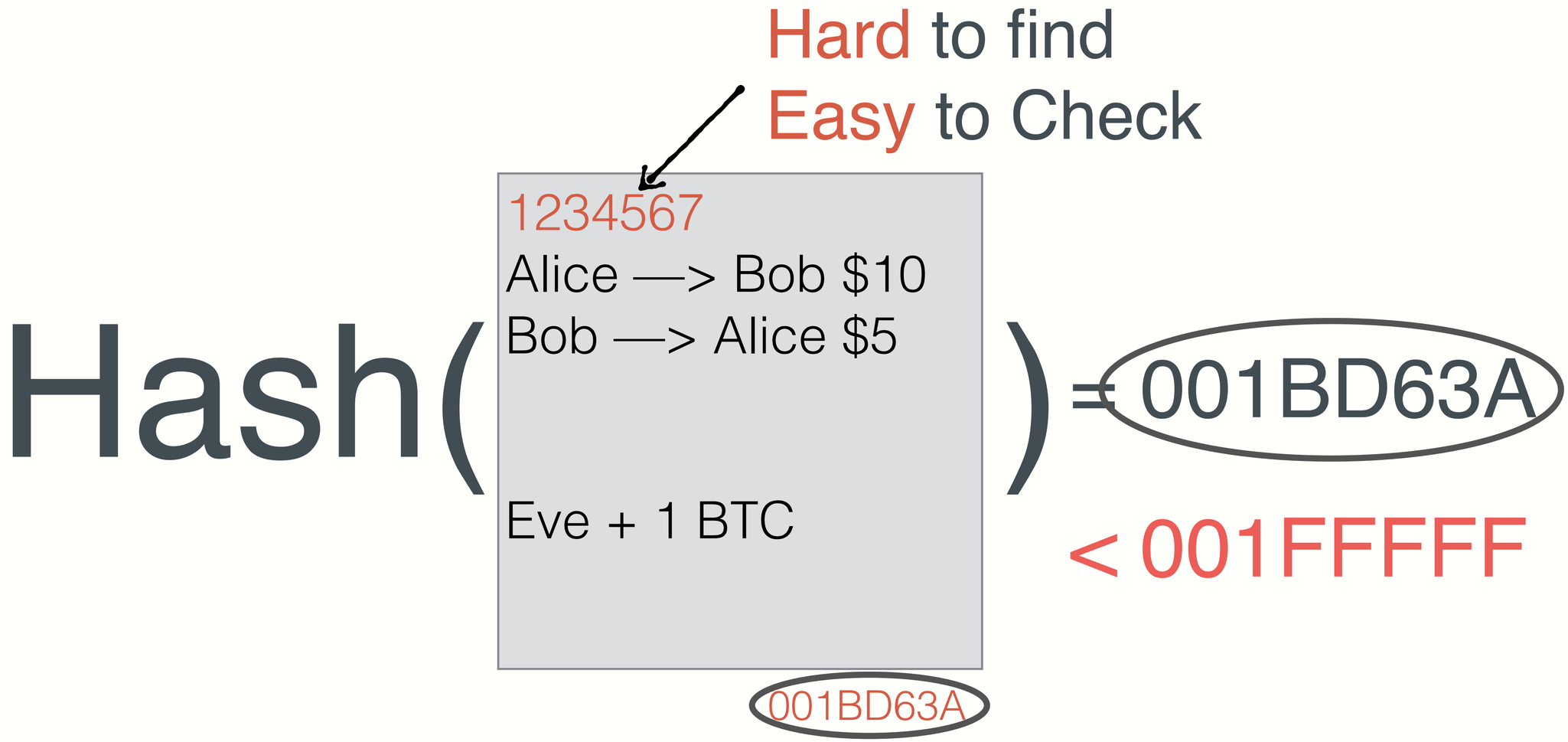


Bitcoin Ming (informal)

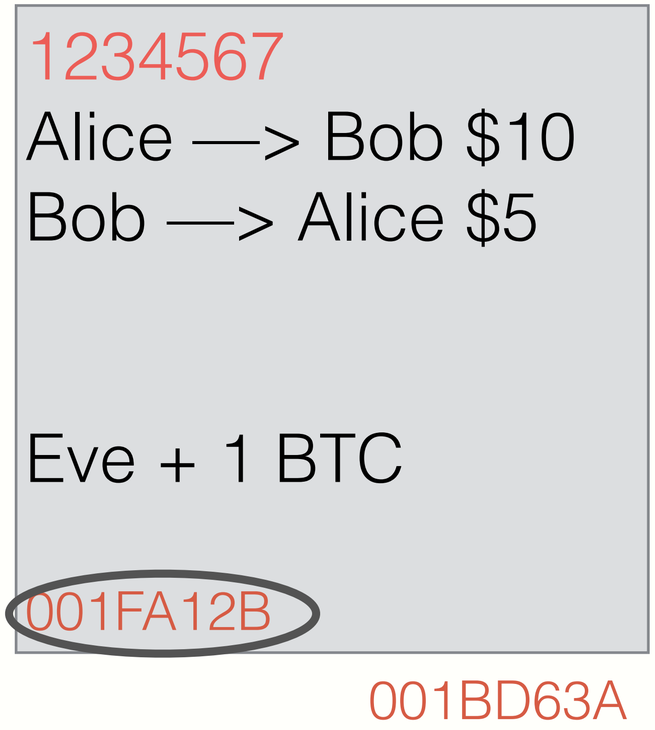


Bitcoin Proof-of-Work

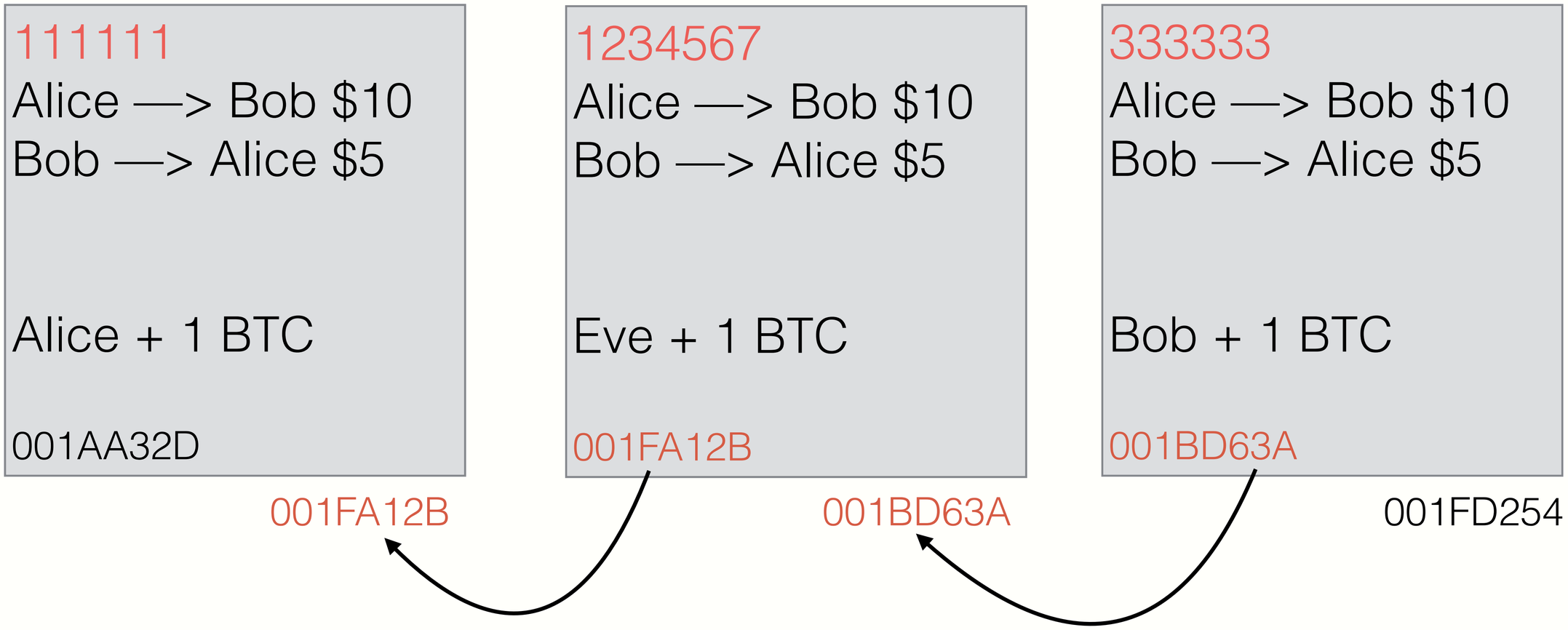
Bitcoin Ming (informal)



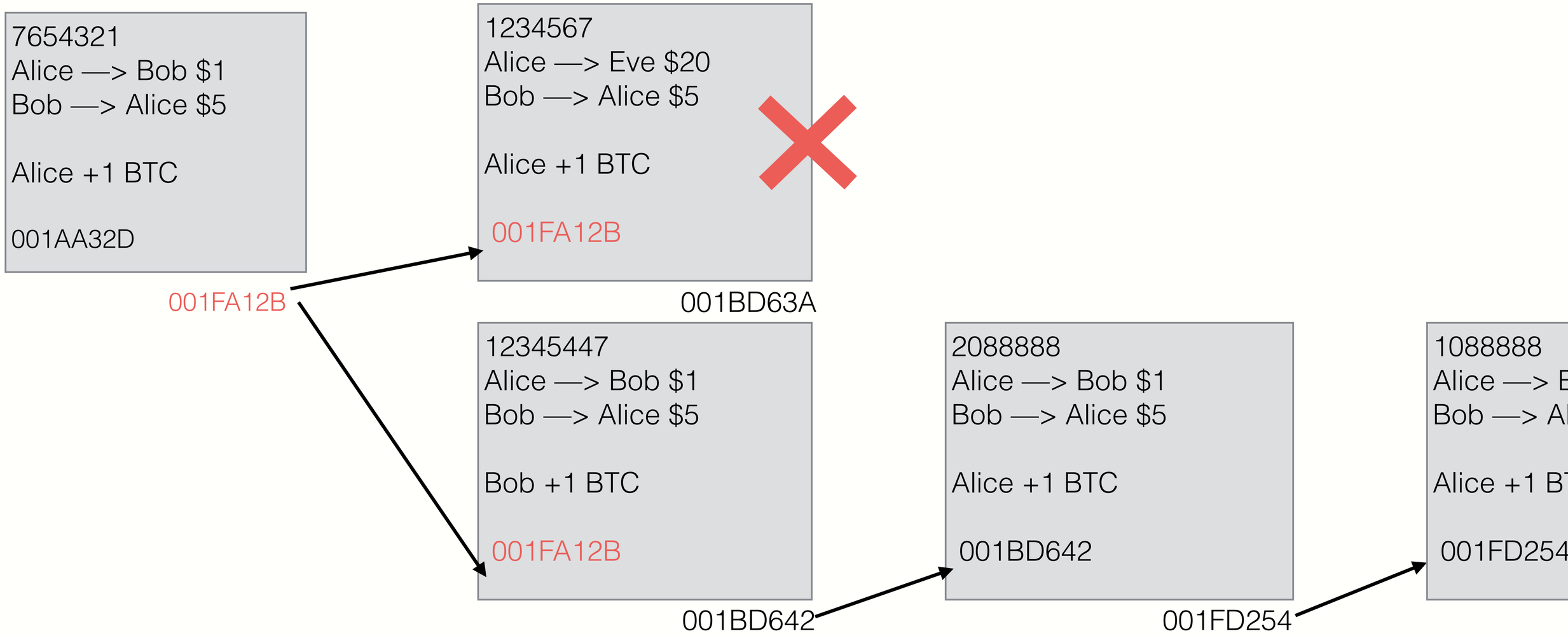
A Bitcoin Block (informal)



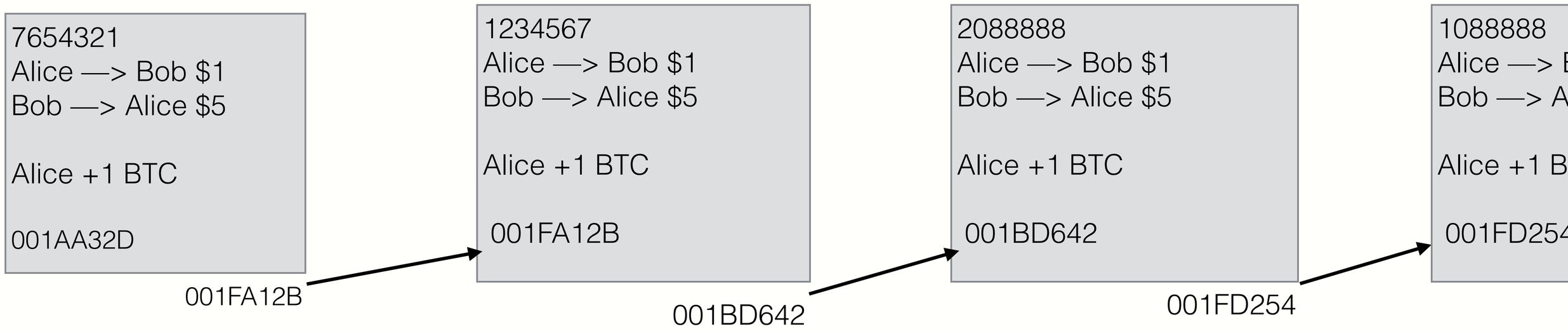
A Bitcoin Blockchain (informal)



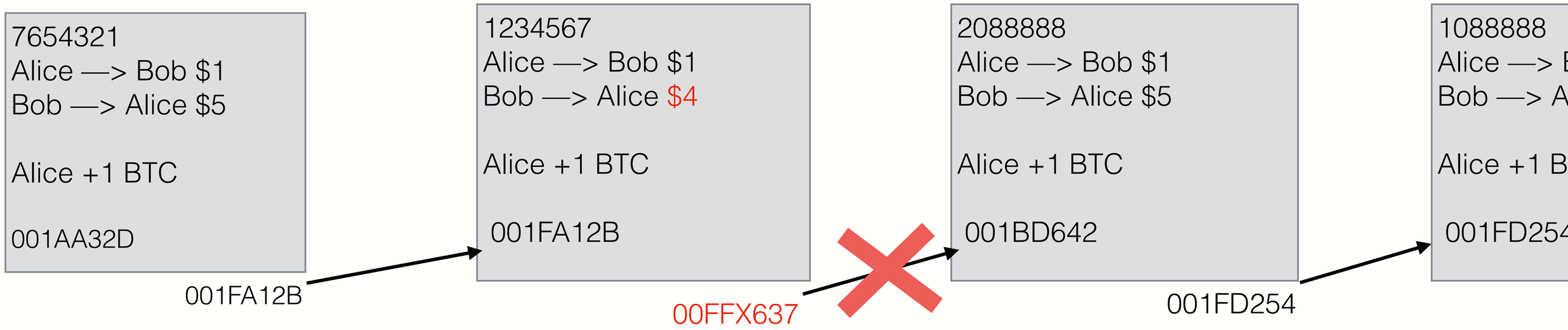
Bitcoin Blockchain Consensus Protocol (informal)



Immutable


7654321
Alice —> Bob $1
Bob —> Alice $5
Alice +1 BTC
001AA32D
001FA12B
1234567
Alice —> Bob $1
Bob —> Alice $5
Alice +1 BTC
001FA12B
001BD642
2088888
Alice —> Bob $1
Bob —> Alice $5
Alice +1 BTC
001BD642
001FD254
1088888
Alice —> B
Bob —> A
Alice +1 B
001FD254

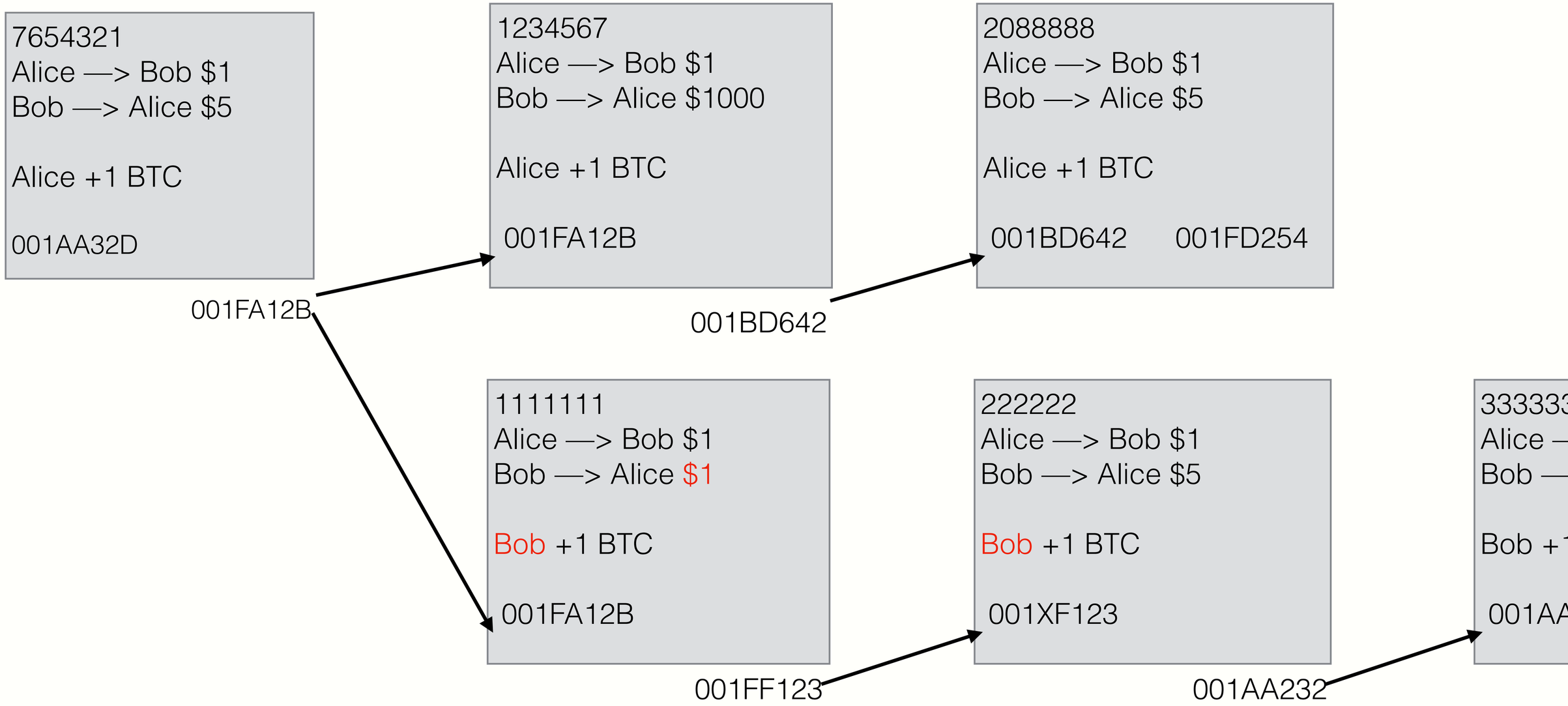
Immutable


7654321
Alice —> Bob $1
Bob —> Alice $5
Alice +1 BTC
001AA32D
001FA12B
1234567
Alice —> Bob $1
Bob —> Alice $4
Alice +1 BTC
001FA12B
00FFX637
2088888
Alice —> Bob $1
Bob —> Alice $5
Alice +1 BTC
001BD642
001FD254
1088888
Alice —> B
Bob —> A
Alice +1 B
001FD254

Immutable

Except for 51% Attack

51% Attack


7654321
Alice —> Bob $1
Bob —> Alice $5
Alice +1 BTC
001AA32D
001FA12B
1234567
Alice —> Bob $1
Bob —> Alice $1000
Alice +1 BTC
001FA12B
001BD642
2088888
Alice —> Bob $1
Bob —> Alice $5
Alice +1 BTC
001BD642 001FD254
1111111
Alice —> Bob $1
Bob —> Alice $1
Bob +1 BTC
001FA12B
001FF123
222222
Alice —> Bob $1
Bob —> Alice $5
Bob +1 BTC
001XF123
001AA232

Evolution of Blockchains

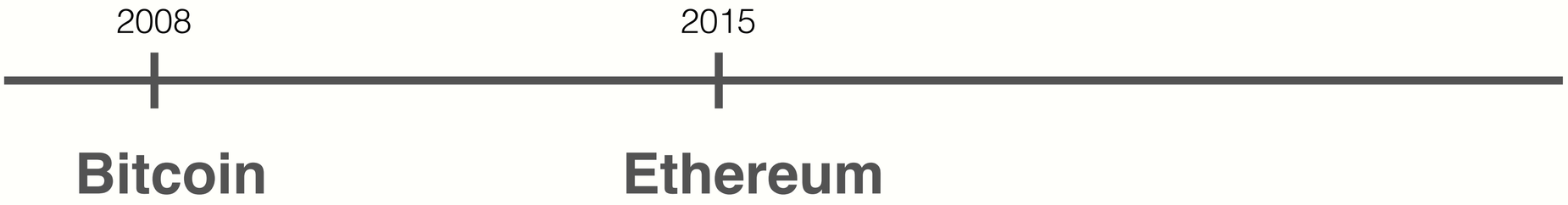
2008

Bitcoin

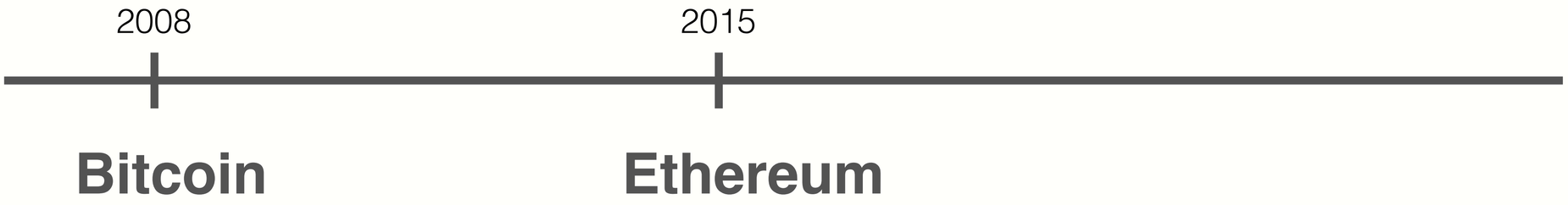
- A public append-only data structure, secured by replication and incentives
- No trusted party
- A fixed supply asset

- Supports stack-based programs

Evolution of Blockchains



Evolution of Blockchains



- **Blockchain computer:** a fully programmable environment (for smart contracts)
- **Composability**: applications running on chain can call each other
- **Consensus**: from Proof-of-Work to Proof-of-Stake

Evolution of Blockchains

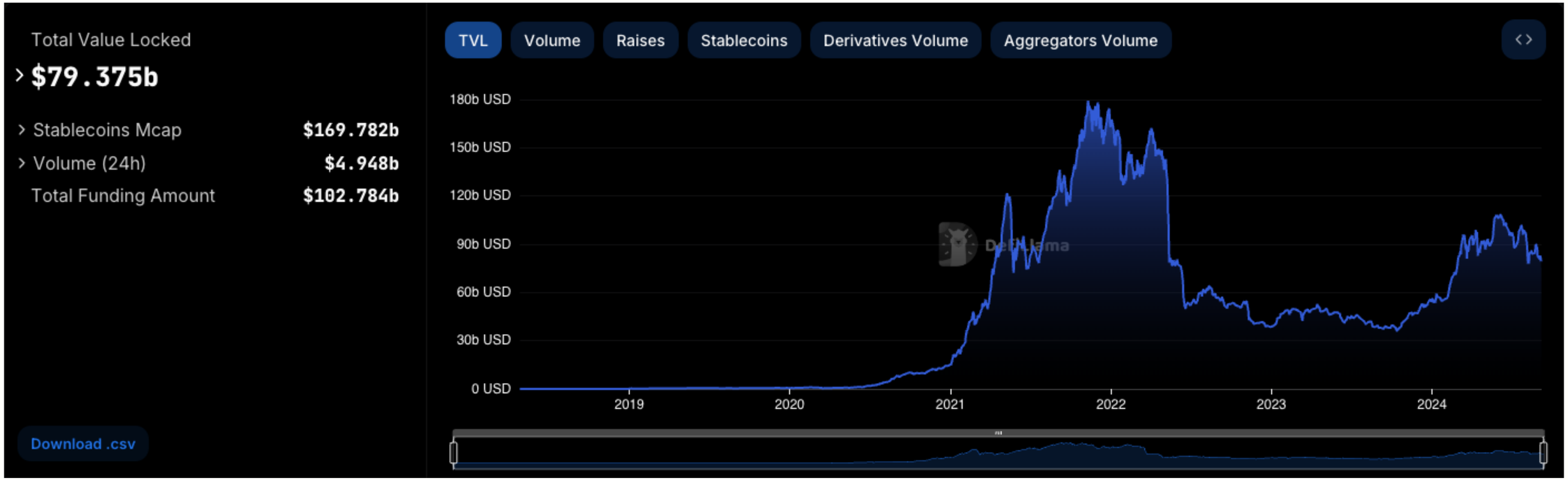
- **DeFi:** financial instruments managed by public program, e.g., stablecoins, lending, DEX, …
- **Asset Management (NFTs)**: art, game assets, domain names, …
- **Decentralized Organizations (DAOs)**: for investment, donations, …

Total Value Locked in DApps (2024.09.05)

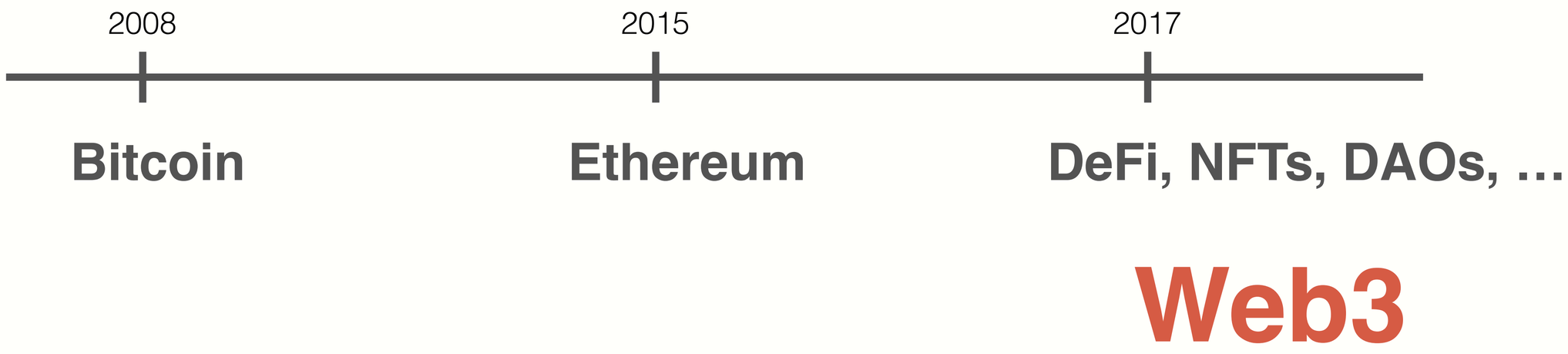
2008 — **Bitcoin**

2015 — **Ethereum**

2017 — **DeFi, NFTs, DAOs, …**



Total Value Locked in DApps (2024.09.06)



2 Bite Size Web3

Web1 (1990-2005)

Web1

Read-only

Web2 (2005-2020)

Web2

Read

Write

Web3 (2020-now)

Web3

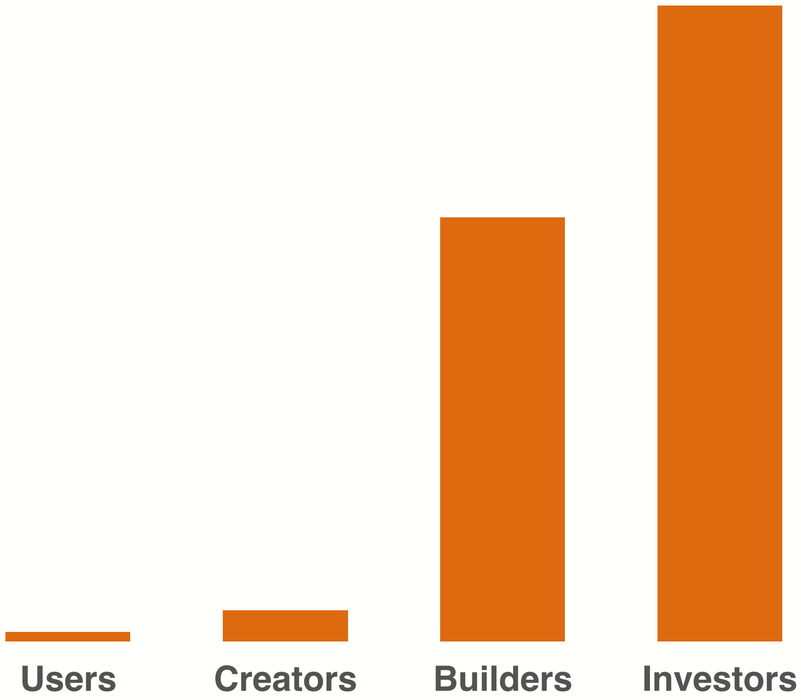
Read

Write

Own

ethereum

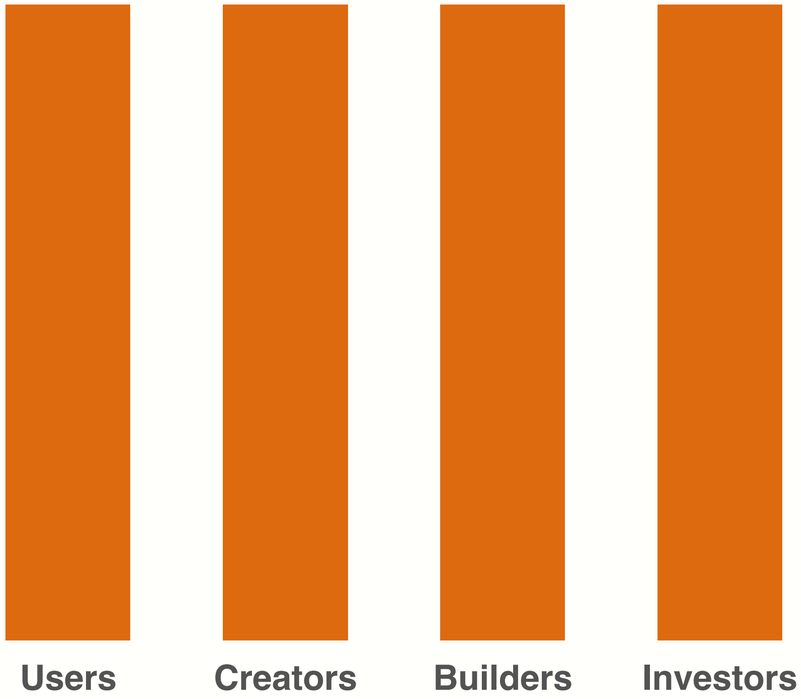
Web2 (2005-2020)



Web2’s value share

Web3 (2020-now)

Through tokens



Web3’s value share

Web3 aligns network participants to work together toward a common goal
— the growth of the network

3 Course Structure

This Course

Blockchain and Web3 concepts

Blockchain and Web3 engineering practices

Designed for:

- Aspiring entrepreneurs excited to build Web3
- Aspiring engineers/researchers who want to get started on Web3

Similar to a Web3 startup incubator
DO NOT take if you are not comfortable with an experimental course

This Course

Main Lectures on blockchain and Web3 concepts and practices

Guest Lectures by investors and builders in Web3

Presentations by YOU

Discussion sessions on how to run a startup

Tentative Main Lecture Topics

- Bitcoin mechanics
- Consensus protocols
- Ethereum and decentralized applications
- Economics of decentralized applications
- Private transactions on a public blockchain (zkp)
- Security of decentralized applications
- Scaling the blockchain
- …

Course Organization

- A final project done in groups of 4-6 students

- No assignments
- No exams

The Team Project Deliverables

- Preliminary project proposal: 10% (Sept 19)
- Project proposal (and presentation): 20% (Oct 17)
- Minimum viable product: 20% (Nov 14)
- Final project report (and presentation): 50% (Dec 05)

Teams

- Immediately start forming teams (4 to 6)
- Each member should participate in design, coding, and documentation

How Do You Work In a Team

- Address problems sooner rather than later
  If you think your teammate's a flake, you're right
- Complain to me or your TA as early as possible
  Alerting me a day before the project is due isn't helpful
- Not every member of a team will get the same grade

First Three Tasks

- Decide who you will work with
  You'll be stuck with them for the term; choose wisely
- Assign a role to each member
- Select a weekly meeting time
  Harder than you might think

Preliminary Project Proposal

- Describe roles of each team member
- Briefly describe the project that you plan to implement
- 1 page
- Due: Sept 19

4

Discussion Session

How to start a startup?