What are Blockchains and what are they good for?

Dan Boneh

Stanford University

Cryptography: application areas

Traditional applications of Cryptography: **Internet Security**

⇒ secure communication: encryption, key exchange, etc.

More recent applications of Cryptography: **Blockchain systems**

⇒ data integrity: signatures, commitments, ZK proofs, …

⇒ Protecting secret keys via threshold signatures (MPC)

The Science of Blockchains (conference, aug. 2023)

Blockchains are a major driver for new technology:

- New consensus protocols (distributed systems)
- New cryptography
- New economic models (tokenomics, lending protocols, exchanges)
- New democratic governance mechanisms (DAOs)
- New programming languages and verification tools

What are blockchains for?

Short answer: a blockchain provides a method

to coordinate among many parties

when there is no single trusted party

if trusted party exists ⇒ no need for a blockchain

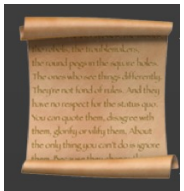
[financial systems: often no trusted party]

Current application areas

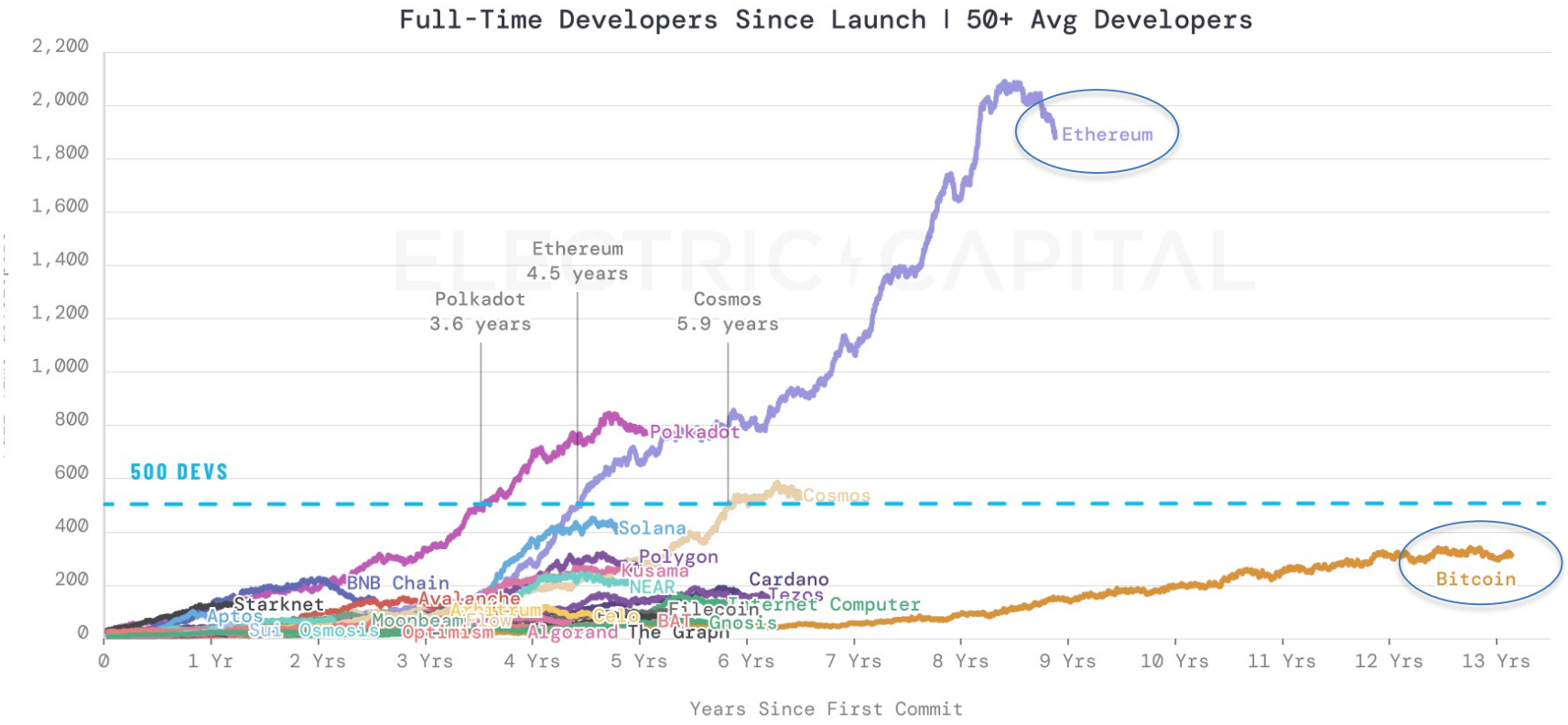
1. **Finance** (DeFi):
   - new financial instruments, exchanges, lending, …

2. Managing **digital assets** (NFTs)
   - Assured provenance

3. **Decentralized organizations** (DAOs):
   - DAOs for investment, for donations, for collecting art, etc.
   - Governance: group decision making



Active developers since launch (as of 12/31/2021)



source: electric capital

This course

A quarter-long course in four days:

- Today: Introduction to blockchains
- Day 2: Proof systems: how they work and what are they for
- Day 3: Consensus protocols
- Day 4: DeFi and user facing tools

Blockchains

Blockchains: what is the new idea?

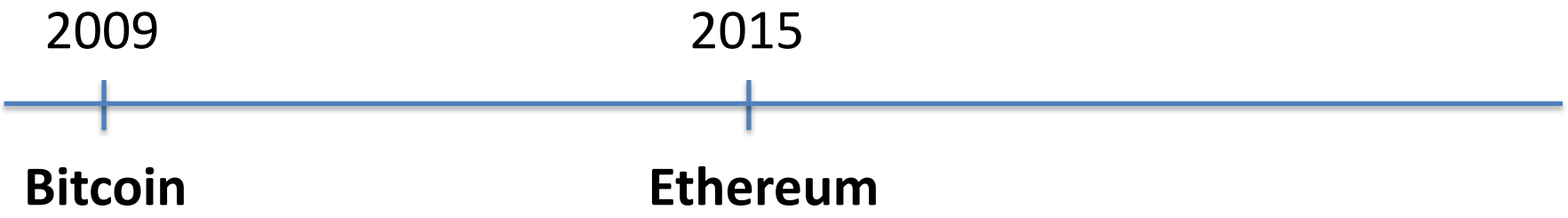
2009

Bitcoin

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?



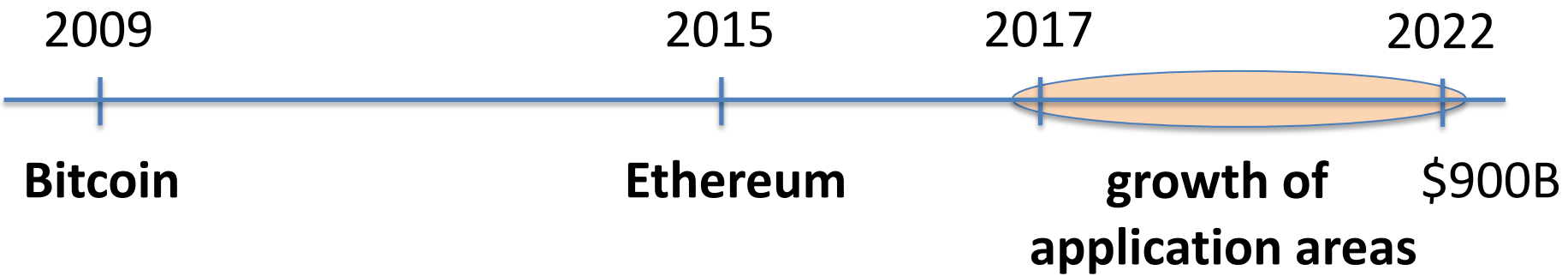
Several innovations:

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

  $\Longrightarrow$ public programs that manage digital and financial assets

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

Blockchains: what is the new idea?



What is a blockchain?

user facing tools (cloud servers)

applications (DAPPs, smart contracts)

execution layer (blockchain computer)

consensus layer / data Availability

Consensus layer (informal)

A public replicated data structure (ledger) that provides:

- **Safety**: all honest participants have the same data *

  ⇒ **Persistence**: once added, data can never be removed

- **Liveness:** honest participants can add new transactions **

  ⇒ **Censorship resistance**: anyone can add data

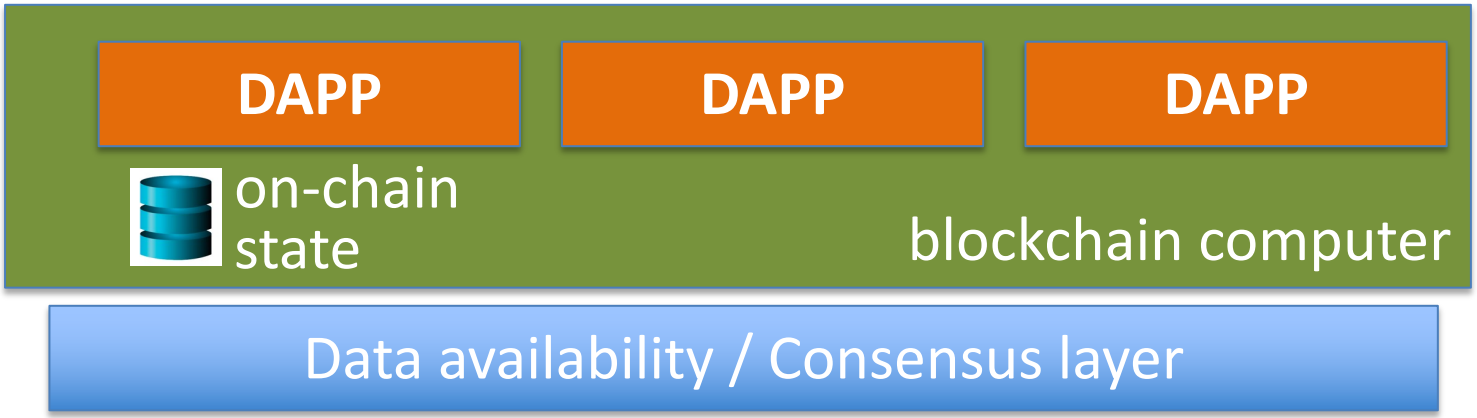
(more in the next lecture)

consensus layer / data availability

Next layer: the blockchain computer

Decentralized applications (DAPPs):

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

Assets managed by DAPPs

MakerDAO	Ethereum	StableCoin	$7.30B
Curve	Ethereum	Exchange	$4.60B
Aave	Ethereum	Lending	$4.09B
Uniswap	Ethereum	Exchange	$3.73B
Compound	Ethereum	Lending	$2.23B

source: defillama

Sep. 2022

Two application areas (briefly)

(1) Decentralized Finance (DeFi)

- **Permissionless**: any financial instrument can be implemented and deployed with a few lines of Solidity code

- **Transparent**: Dapp code and Dapp state are public

  $\Longrightarrow$ Anyone can inspect and verify

- **Composable**: Dapps can call one another

  ERC-20 standard enables interoperability (6 functions)

Why DeFi? Failures of the existing financial system

- **Cross border inefficiency**: send $10 to south america ⇒ 36% fees

- **Economies with an unstable fiat currency**

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

- **The high cost of being poor in america:**

  In 2019, **5.4 percent** of US households were unbanked

Is this good or bad?

DeFi optimist:

DeFi is a technological advance that enables easy access to the financial system to anyone with an Internet connection, offering new capital efficiencies.

DeFi pessimist:

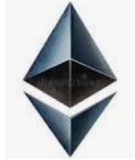
An unregulated, hack-prone system, that enables novel forms of financial crime.

Which is right ??

More in lecture 4 today

Application (2): Decentralized Orgs (DAO)

What is a DAO?



- A Dapp deployed on-chain at a specific address
- Anyone (globally) can send funds to DAO treasury
- Anyone can submit a proposal to DAO
  - ⟹ participants vote
  - ⟹ approved ⇾ proposal executes

snapshot.org

Examples of DAOs

- There are over 12000 DAOs managed on Snapshot
- **Collector DAOs**: PleasrDAO, flamingoDAO, ConstitutionDAO, …

  (see art collection at https://gallery.so/pleasrdao)

PleasrDAO: 103 members.

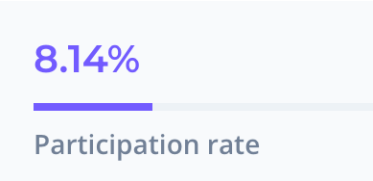
Manages a treasury, has full time employees.

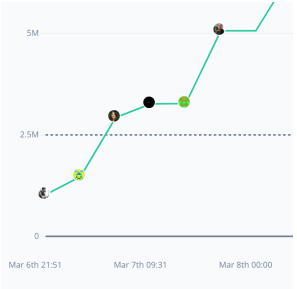
Deliberations over what to acquire over telegram.

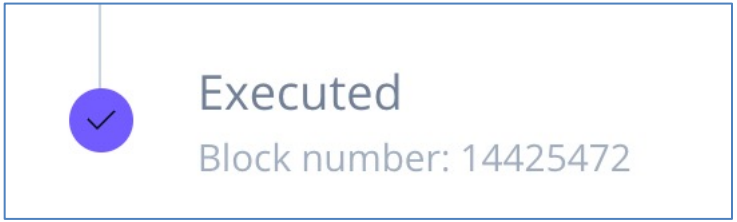
Examples of DAOs

- There are over 12000 DAOs managed on Snapshot
- Collector DAOs: PleasrDAO, flamingoDAO, ConstitutionDAO, …
- **Grants DAOs**: gitcoin (83K members), …

Proposal ID 21: This proposal looks to ratify the allocation of 30,000 GTC from the Community Treasury to the MMM workstream.







(tally.com)

Examples of DAOs

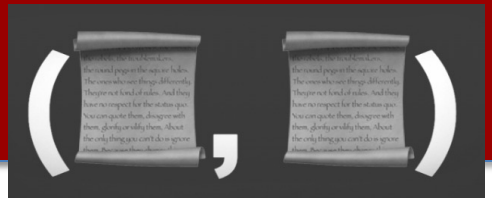
- There are currently about 12000 DAOs managed on Snapshot
- Collector DAOs: PleasrDAO, flamingoDAO, ConstitutionDAO, …
- Grants DAOs: gitcoin, …
- **Protocol DAOs**: manages operation of a specific protocol
  Uniswap DAO (74K), Compound DAO (8K), …
- **Social DAOs**: FWB, …
- **Investment DAOs**: many

Many DAO governance experiments

Who can vote? How to vote? What voting mechanism?

DAOs: a platform for experimenting with governance mechanisms

Private DAO treasury



2021: an auction for a physical copy of the constitution

(Sotheby's auction house)

ConstitutionDAO:

- Formed in Nov. 2021 to participate in auction.
- Raised $46.3M from about 20K participants from around the world
- Lost to another bidder who bid $43M

bidder knew that ConstitutionDAO could not outbid it

How to participate in an auction when everyone knows your treasury??

Private DAO treasury

medium.com/@boneh

A simple design:

- A single Ethereum DAPP manages many DAOs (e.g., JuiceBox)
- **DAO manager**: sets up a DAO by publishing a DAO public key

$$pk_{\text{DAO}} = (P, Q), \quad Q = \alpha P; \qquad sk_{\text{DAO}} = \alpha$$

- **Contributor**: sends funds to DAPP with a "blinded DAO pk" : $(\rho P, \rho Q)$
- DAPP records contribution
  - ⇒ an observer learns nothing about which DAO received the funds
  - ⇒ only learns *total* amount stored on the platform as a whole
- DAO manager can later use its secret key α to claim funds sent to its DAO

Many other DAO privacy questions …

- **Private DAO participation**: keep membership list private
- **Private voting**: keep who voted how on each proposal private
- **Privately delegate** voting rights

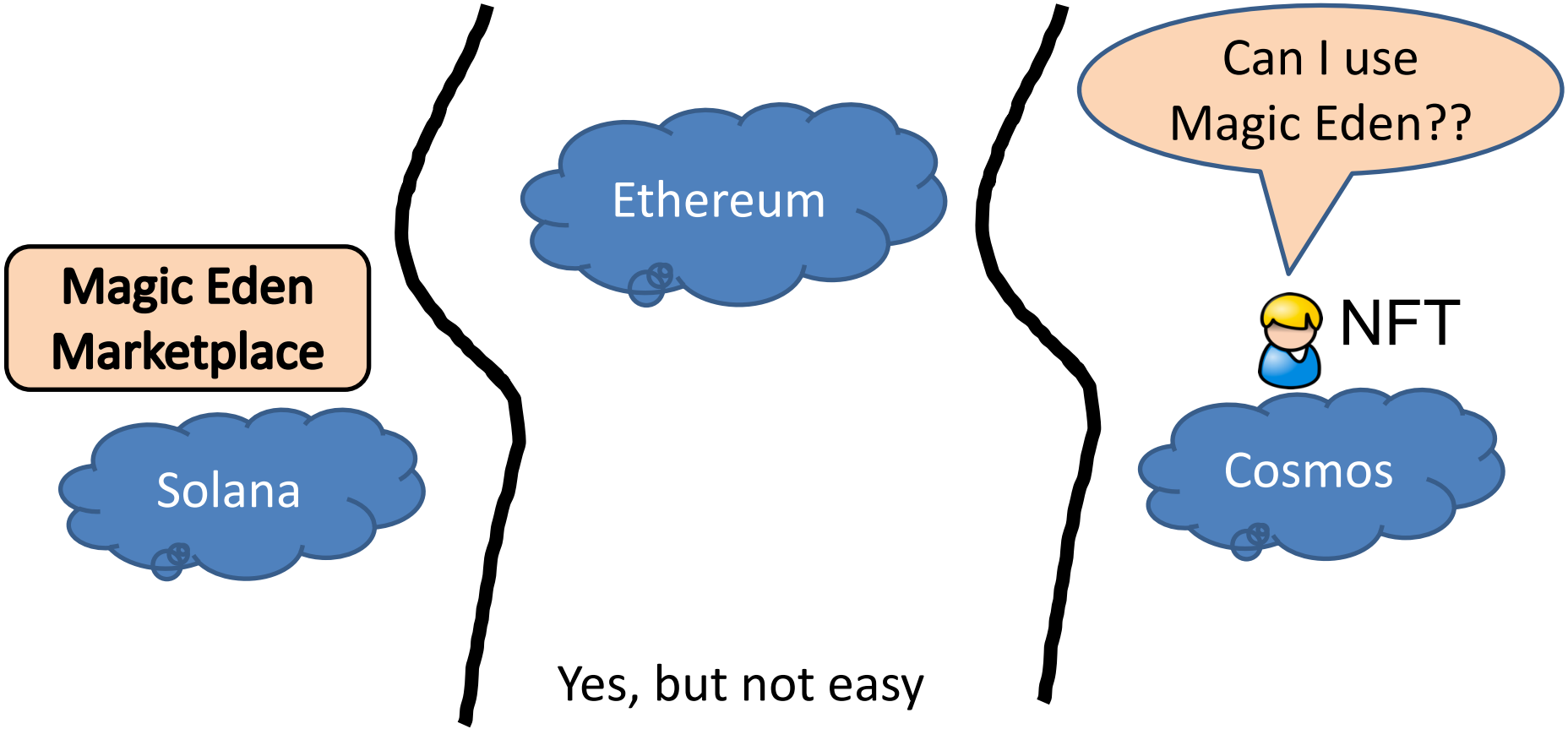
… while complying with all relevant laws.

Some of these questions are solved by
general privacy platforms such as **Aztec**, **Aleo**, and others.

Many more hot research topics

- **Scaling the blockchain** (tomorrow)
- **Privacy on the blockchain**
  - Businesses cannot use if all transactions are public
- Efficient **interoperability** between blockchains
- Managing **Maximal Extractable Value (MEV)** [Day 4]
- Zero knowledge proofs of solvency

The interoperability problem



THE END

Next topic: an introduction to consensus protocols