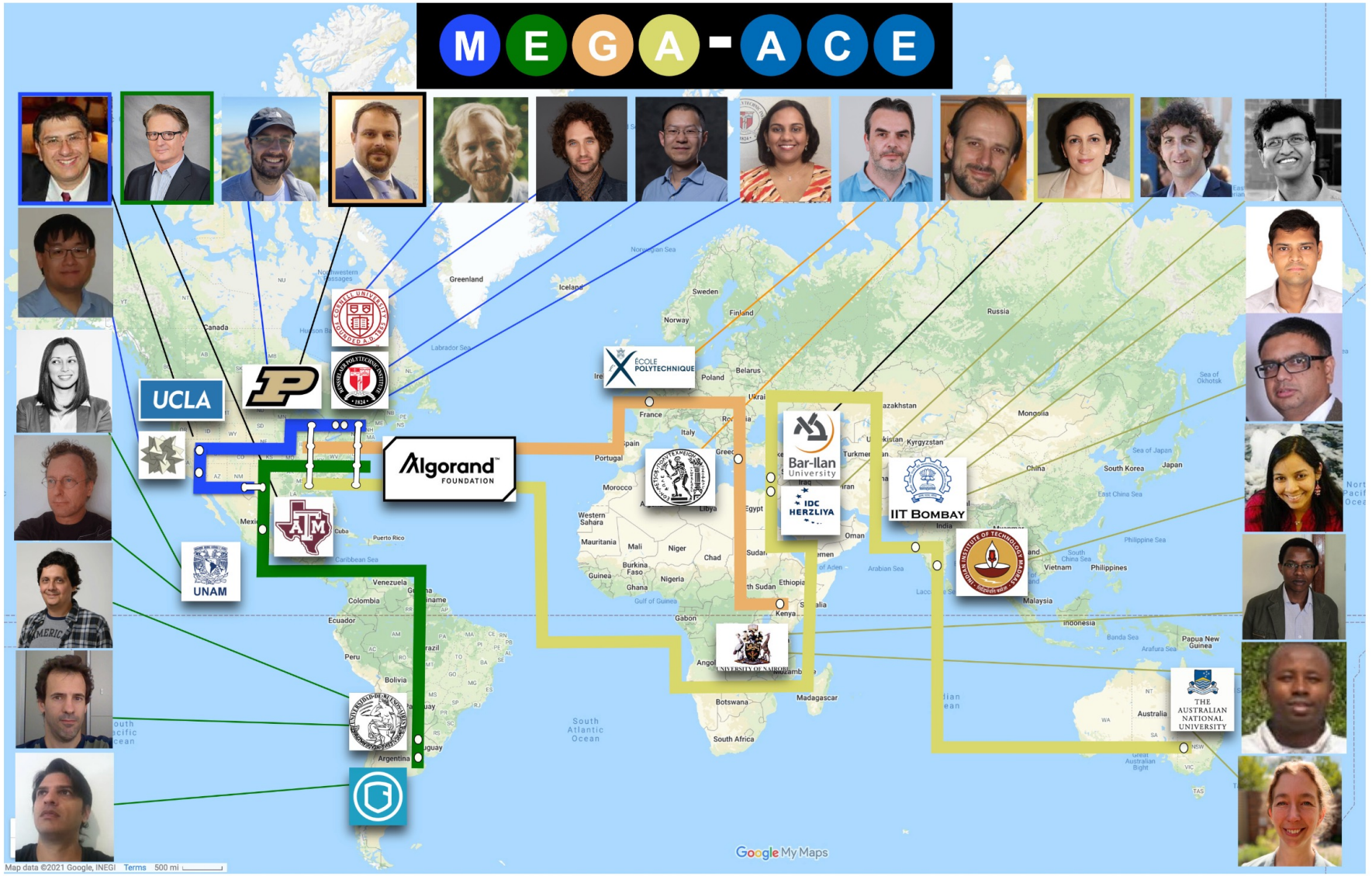
Inaugural Texas A&M Blockchain Day

Welcome & Blockchain Warm-Up

Juan Garay
Department of Computer Science & Engineering
Texas A&M University
garay@tamu.edu
https://jagaray.com

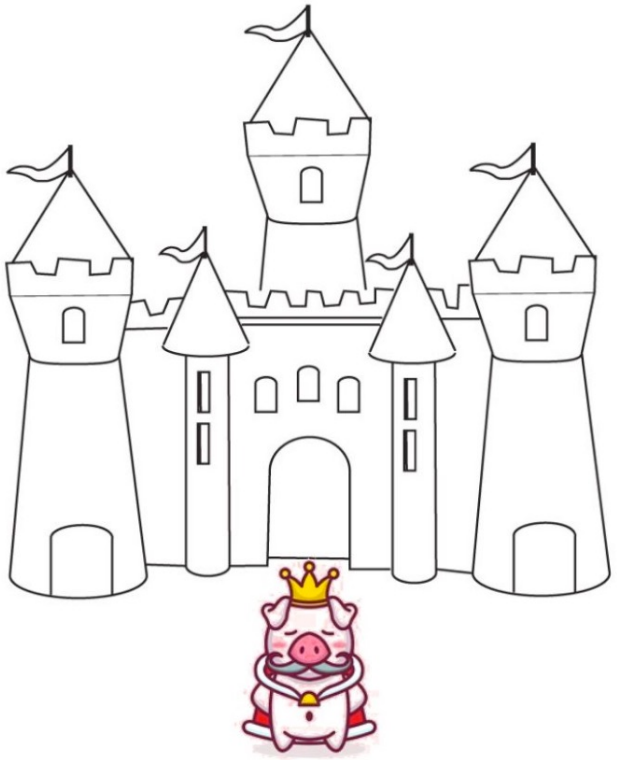
Event Sponsors

MEGA-ACE: Multidisciplinary Educational Global Alliance for Algorand Center of Excellence



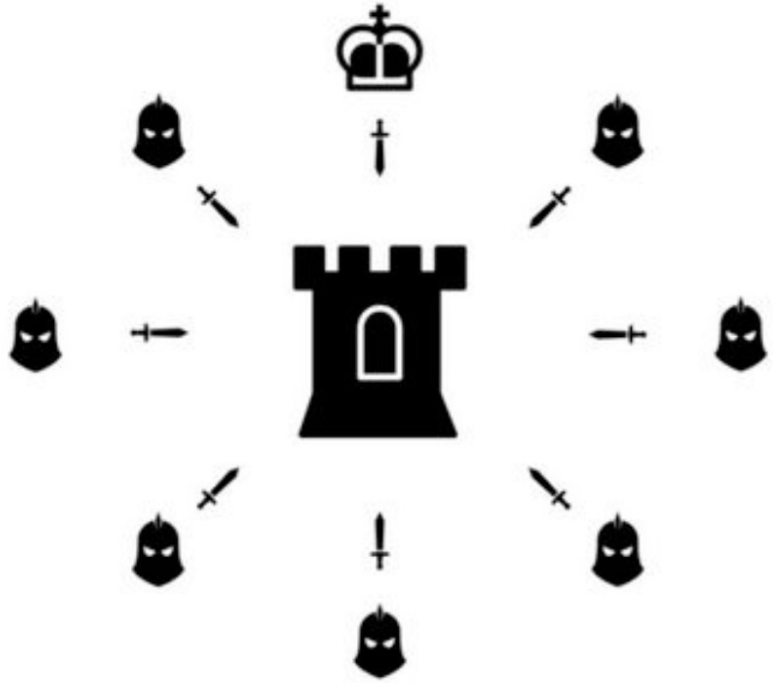
Centrally Controlled (Computer) Systems

- A single person (party/node) controls who can read/write/delete data
- If the person/party/node dies/is dishonest/crashes, the system crashes



Controlled-Access Distributed Systems

- Nodes collectively control the system
- If only few nodes are faulty, system remains operational
- Controlled participation — only authorized parties



Open-Access Distributed Systems?

- Nodes collectively control the system
- If only few nodes are faulty, system remains operational
- Anyone can participate, join or leave as they please

What is a Blockchain?

- A *blockchain* is a distributed database that satisfies a unique set of *safety* and *liveness* properties
- To understand it, we will focus on its first application
- *Distributed ledgers* use a blockchain as one possible means of implementation

Distributed Ledger

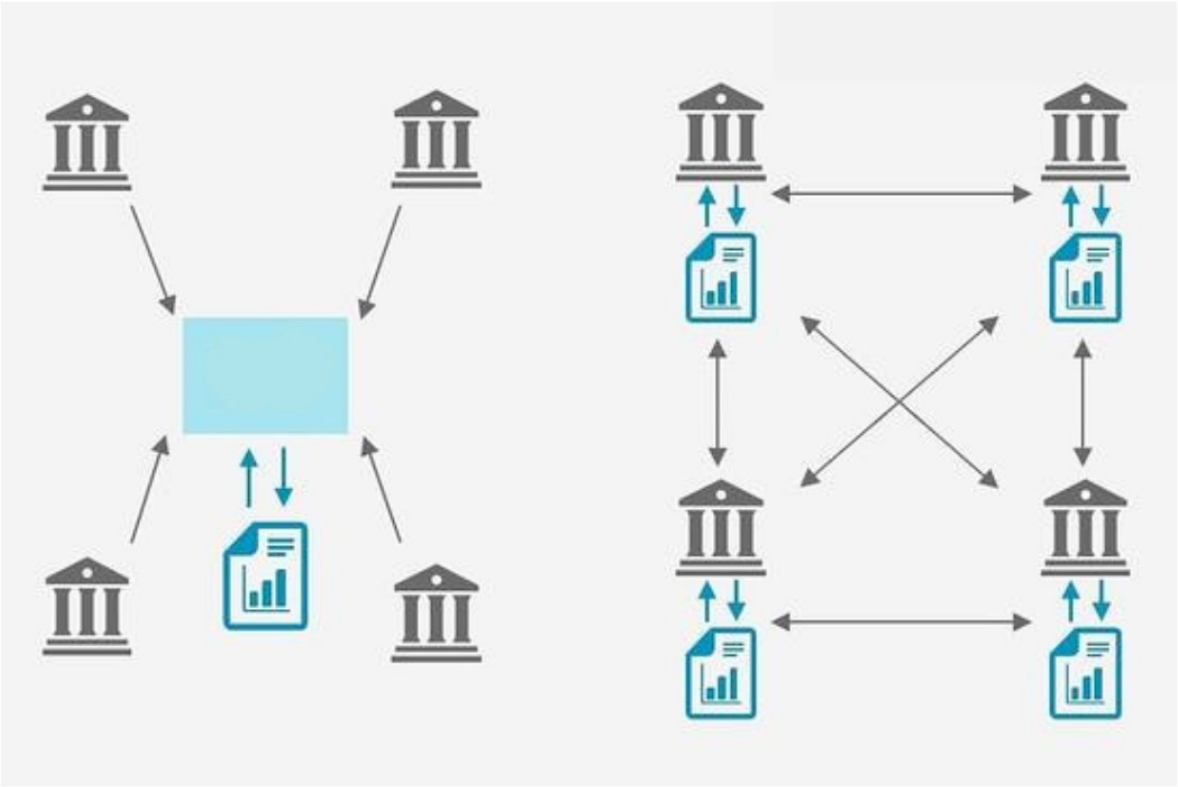


Figure: http://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/

- Consistency: Everyone sees the same history
- Liveness: Everyone can add new transactions

The Never-Ending-Book Parable

A Book of Data

- Anyone can be a scribe and produce a page
- New pages are produced indefinitely, as long as scribes are interested in doing so
- Each new page requires some effort to produce

Importance of *Consensus*

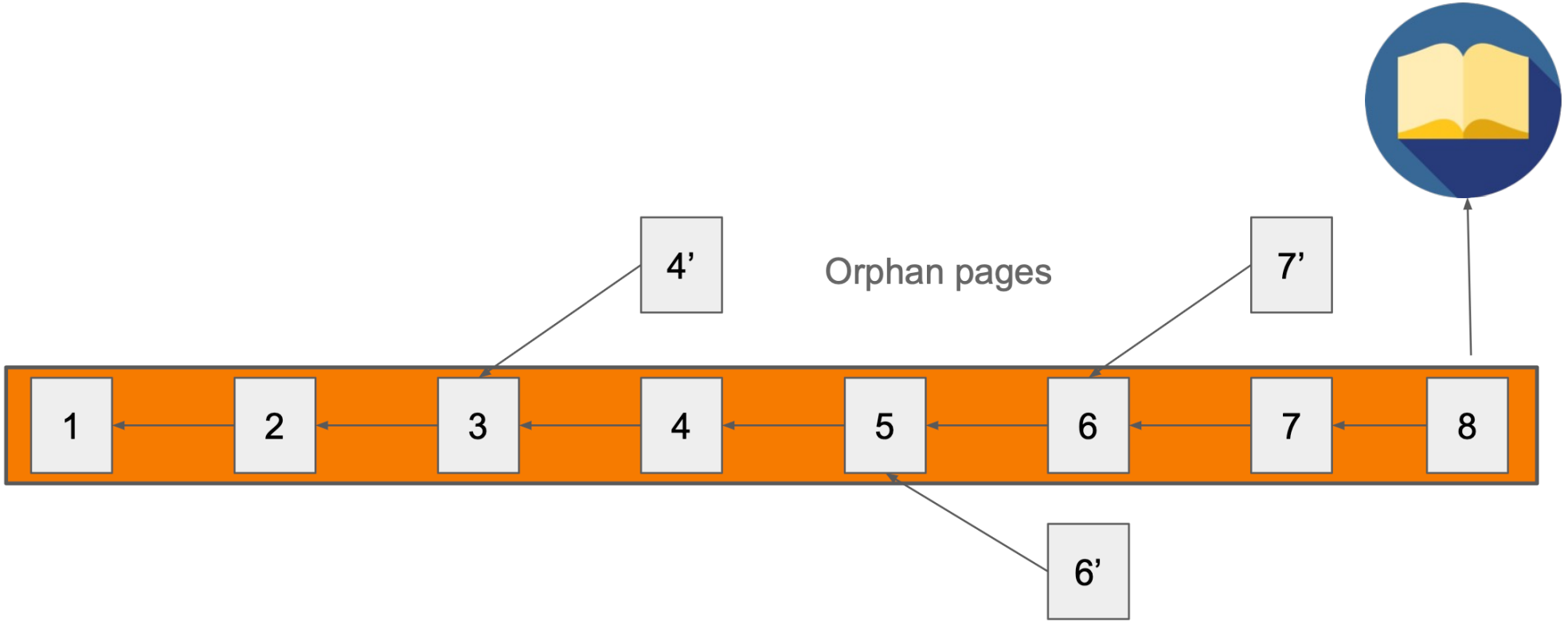
If multiple conflicting books exist, which one is the right one?

Choosing the Correct Book

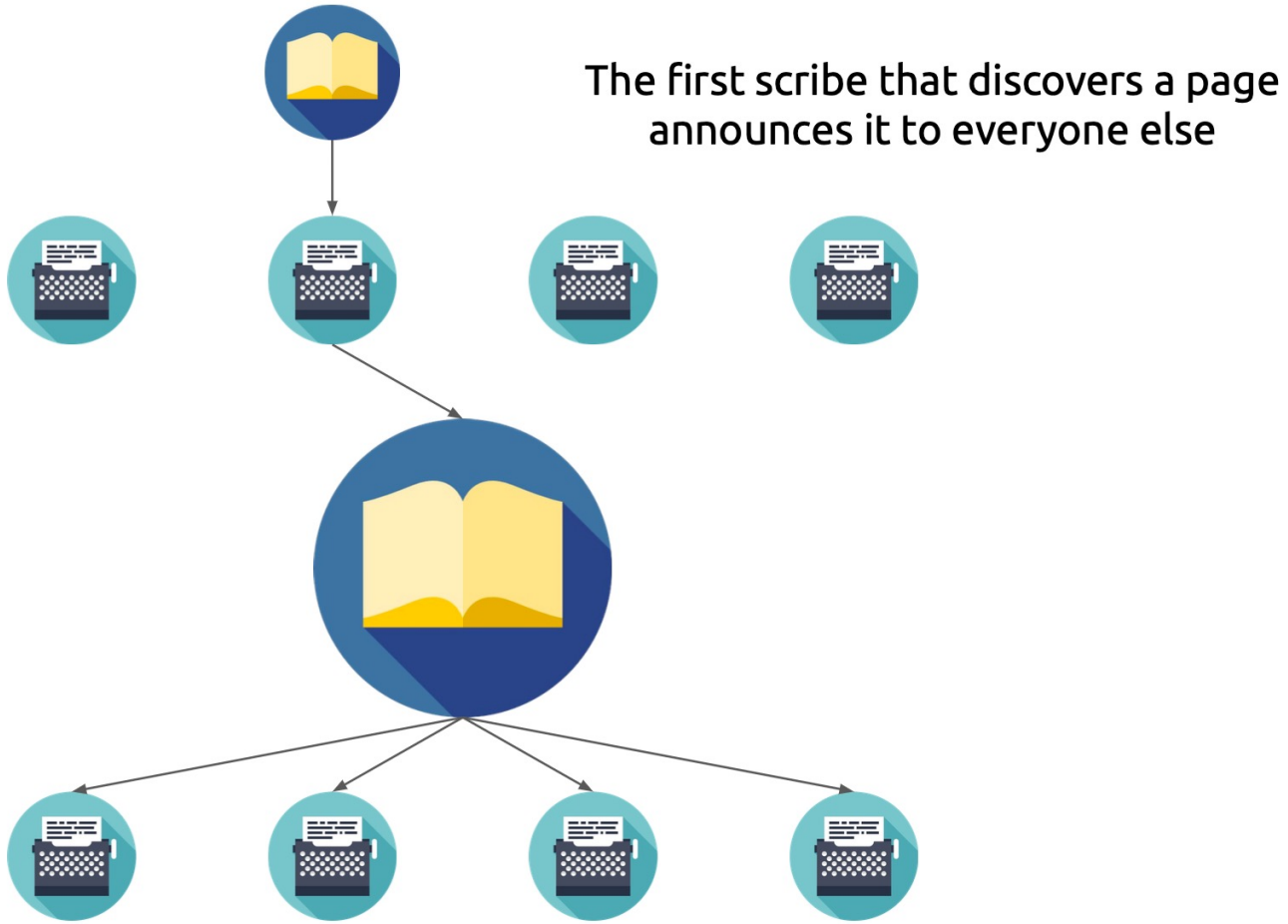
The correct book to work on and refer to is the book with the most pages. If multiple books exist, just pick one at random

Assembling the Current Book

- Each page refers to the previous one
- Assembled by stringing together the longest sequence of pages

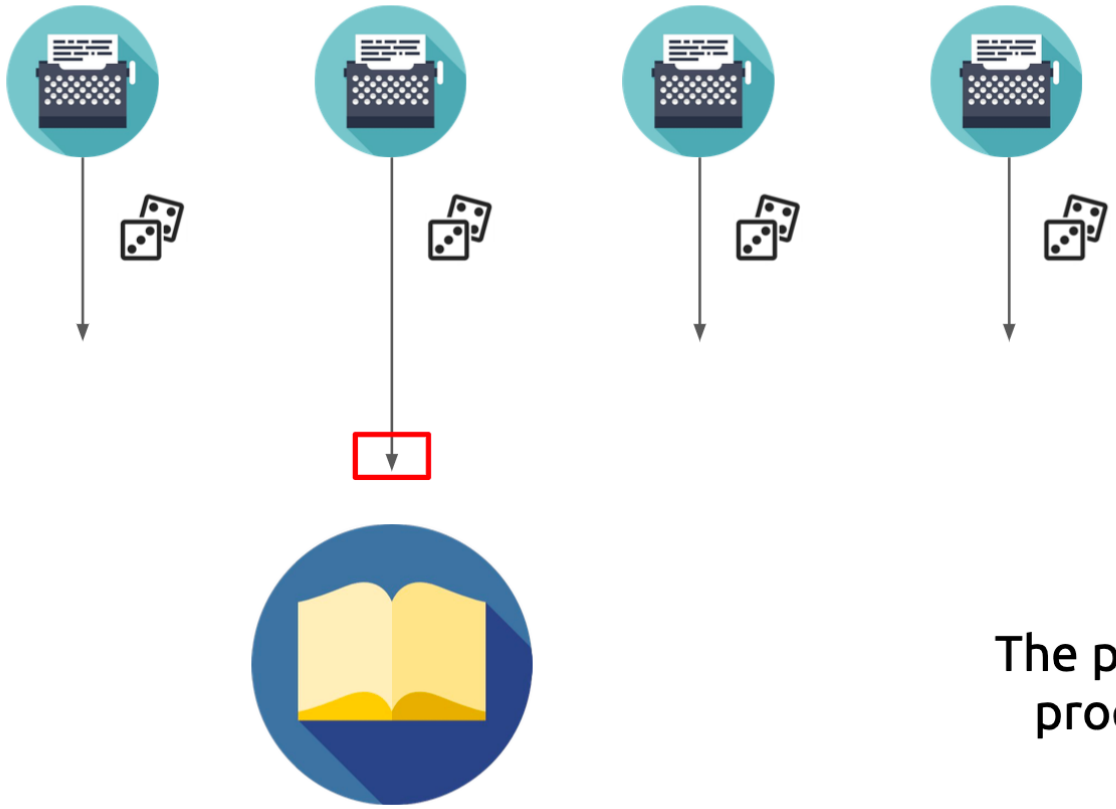


Rules for Adding Pages to (Extend) the Book



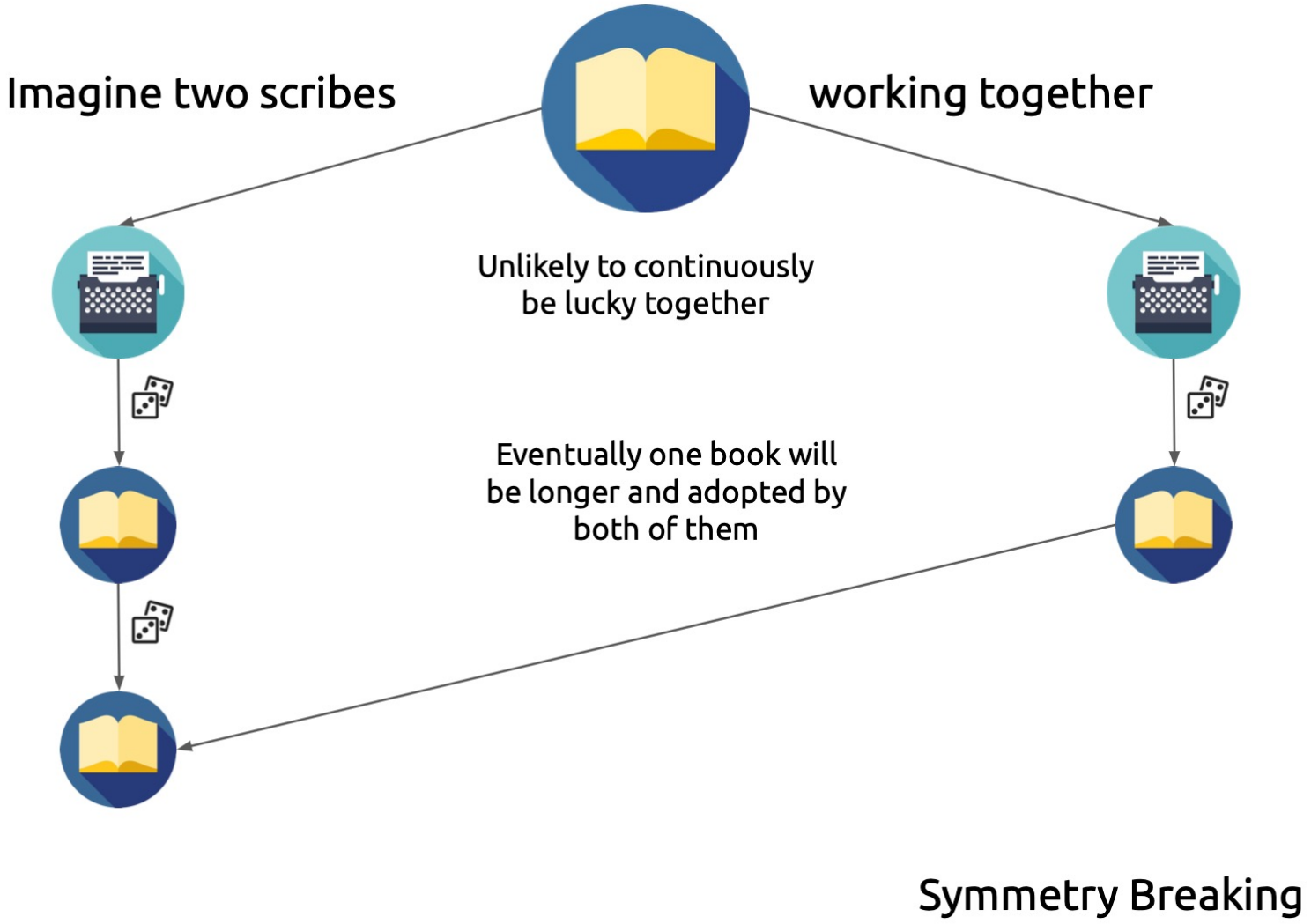
Effort is Needed to Produce a Page

Each page needs a special combination from a set of dice to be rolled



The probabilistic nature of the process is paramount to its security

The Benefits of Randomness



Being a Scribe

- Anyone can be a scribe for the book…
- … as long as they have a set of dice
- The more dice a scribe has, the higher the likelihood to produce the winning combination to add a page to the book

Parable and Reality

	The “blockchain”
	“Miners” / Computer systems that organize transactions in blocks
	Solving a cryptographic puzzle that is moderate hard to solve
	Using a computer to test for a solution from a large space of candidate solutions

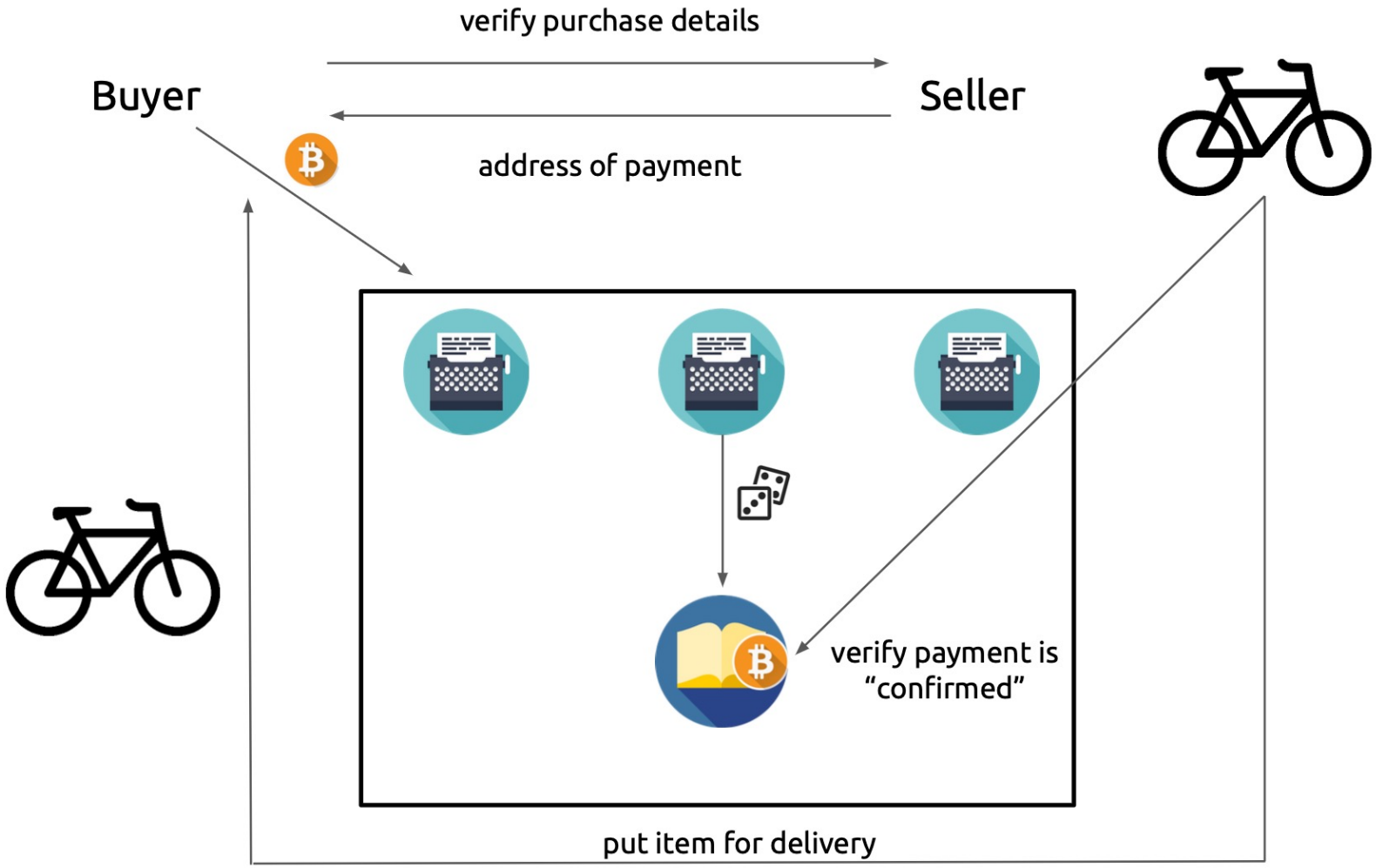
The First Blockchain Application: Bitcoin

What is Bitcoin (Trying to Be?)

- Money
  - Competing with UDS $, GBP £, EUR €, etc.
  - Medium of exchange: Give money to get goods and viceversa
  - Unit of account: Means to price goods, for accounting/debt purposes
  - Short/Medium term store of value: Can be exchanged for the same amount of goods in the (not so distant) future
- Payment system
  - Competing with cash, Visa, Mastercard, etc.
  - High throughput (large no. of transactions/sec)
  - Low latency (fast transaction settlement)
  - Uninterrupted operation
- Commodity
  - Competing with gold, silver, oil, etc.
  - A (useful) “material” that can be bought/sold

Person-to-Person Funds Transfer

Using the Bitcoin “Book”



Advantages

- Resilience
  - The book is shared across the network
  - Even if some of the nodes crash or are corrupted, the system remains operational
- Censorship resistance
  - Anyone can participate
  - Geographical disparity of nodes
  - Good alternative for borderline (or beyond) legal transactions
- Digital and open
  - New applications can easily be built on top of it
  - Programs can be hosted (and executed) on the ledger (“smart contracts”)

Disadvantages

- Bad as money
  - Price fluctuations and circulation do not follow economic growth (bad store of value)
  - Nothing is priced in Bitcoin (bad unit of account)
  - Slow and expensive (bad medium of exchange)
    - Low throughput (~ 5 tx/sec)
    - High latency (~ 60 mins)
    - High fees*** (~ $3)
- Irreversibility
  - If a transaction is processed, it cannot be deleted/reversed
  - If user's Btc's are stolen or user loses key, no recovery mechanism exists
- Environmentally damaging
  - Bitcoin CO_2 footprint*: 76.44 Mt (~Colombia's)
  - *Single* Btc tx CO_2 footprint*: 820.84 kg (~1.8M Visa transactions)
  - Single Btx tx e-waste**: 242 g (1.5 iPhones)

* https://digiconomist.net/bitcoin-energy-consumption

** https://www.sciencedirect.com/science/article/pii/S0921344921005103

*** https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

Smart Contracts

From Money to Smart Contracts

- Since we have created the book, why stop at recording monetary transactions?
- We can encode in the book arbitrary relations between accounts
- Scribes can perform tasks and take action, like verifying that stakeholders comply/adhere to contractual obligations

Questions to Consider

- How are the pages created? Since at the beginning the book is empty, where does the “money” come from? $\Longrightarrow$ Proof of Work (PoW)
- How is it possible to sign something digitally? $\Longrightarrow$ Digital Signatures
- How does a page properly refer to a previous page? $\Longrightarrow$ Hash Functions

Proofs of Work

Proofs of Work (aka “Cryptographic Puzzles”)

- Main objective: Given some *data,* ensure that some effort has been invested in computation involving the data
- “Moderately hard functions” [DN92,RSW96,Back97,JB99,GMPY06, BGJPVW16, BRSV17/18…]

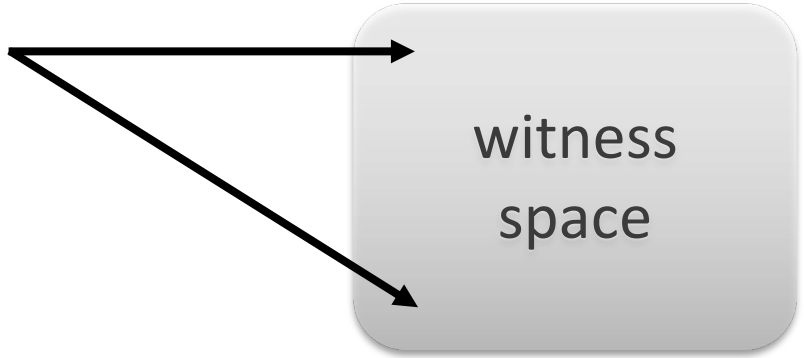
Prover **Verifier**

Proofs of Work (aka "Cryptographic Puzzles") (2)

More formally:

$Q(\cdot,\cdot)$: Polynomial-time predicate

$Q(x,\cdot)$



Challenge determines work level d

Search for witness takes long time (e.g., exp(d)) (a complexity lower bound needs to be assumed)

Successful only with some (small) probability!

Verification is easy!

Proofs of Work (aka "Cryptographic Puzzles") (3)

- One concrete instantiation:

```
int counter;
counter = 0
while Hash(data, counter) > Target
        increment counter
return counter
```

- In this case: PoW of *data* equals a value *w* with the property

$$\text{Hash}(data, w) \leq \text{Target}$$

- In Bitcoin:
  - Hash = SHA-256
  - Example of Target:

Target = 0000000000000000171A8B0000000000000000000000000000000000000000

Questions to Consider

- How are the pages created? Since at the beginning the book is empty, where does the “money” come from? ⟹ Proof of Work (PoW)
- How is it possible to sign something digitally? ⟹ Digital Signatures
- How does a page properly refer to a previous page? ⟹ Hash Functions

Bitcoin Address/Account (Security)

- Based on *elliptic curve cryptography* (ECC, curve *secp256k1*)
- Account: (PrivKey, PubKey)

- Bitcoin address:

  Base58(RIPEMD160(SHA256(PubKey)))

  E.g., *37k7toV1Nv4DfmQbmZ8KuZDQCYK9x5KpzP*

- PrivKey used to **sign** outgoing transactions
- Wallet: many (PrivKey, PubKey)
- Transaction:

Bitcoin Transactions

Example:
Alice sends Bob 1 BTC, Bob uses it to send another payment.

When Alice sends Bob a payment of 1 BTC, she signs a transaction that deducts 1 BTC from her funds and creates a new transaction output that is worth 1 BTC and can only be spent by Bob, the owner of the recipient address.

Bob now wants to send 0.4 BTC to Charles. The transaction output from Alice's transaction is now used to fund this new transaction. The transaction creates two new outputs: One with 0.4 BTC that is associated with Charles' address, and one with 0.6 BTC associated with Bob's address (it is the change). The first transaction output (from Alice's transaction) is consumed by the transaction.

Putting it All Together

PoW-based Blockchain Protocols (Bitcoin)

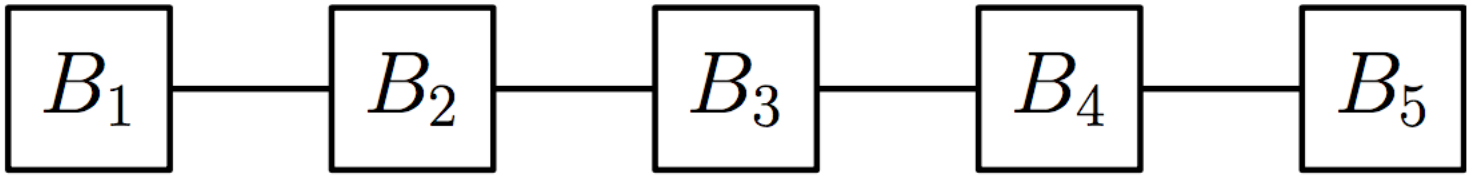
- Parties (“miners”) have to do work in order to install a transaction

PoW-based Blockchain Protocols (Bitcoin)

- Parties (“miners”) have to do work in order to install a transaction
- Transactions are organized in chains of blocks

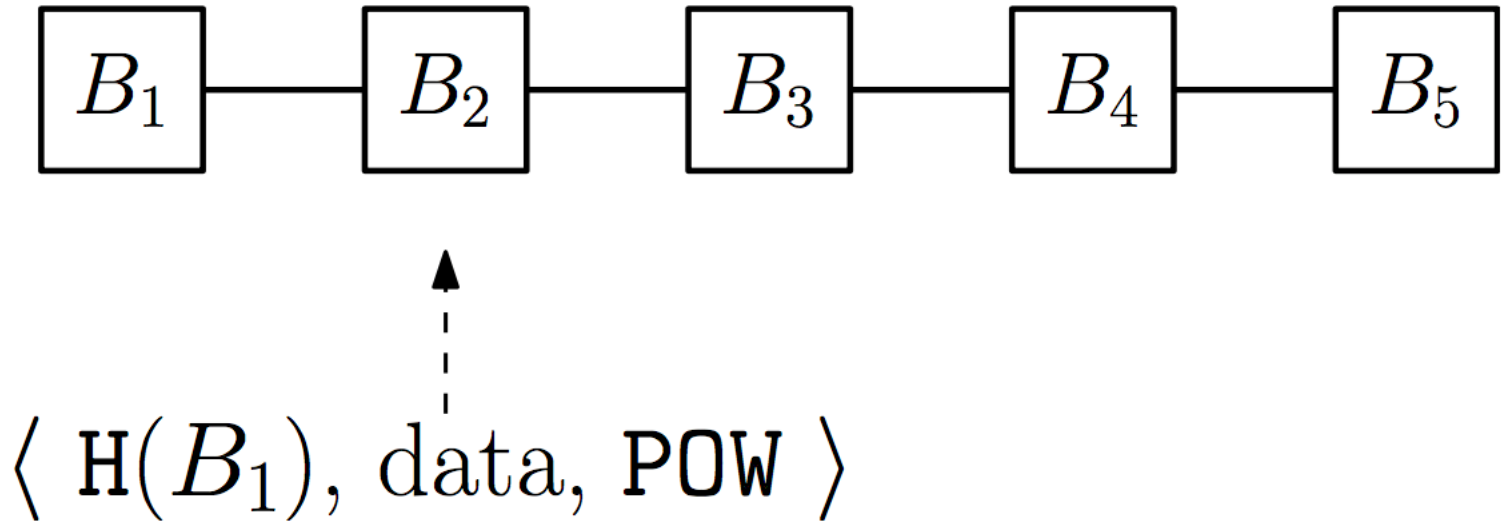
PoW-based Blockchain Protocols (Bitcoin)

- Parties (“miners”) have to do work in order to install a transaction
- Transactions are organized in chains of blocks



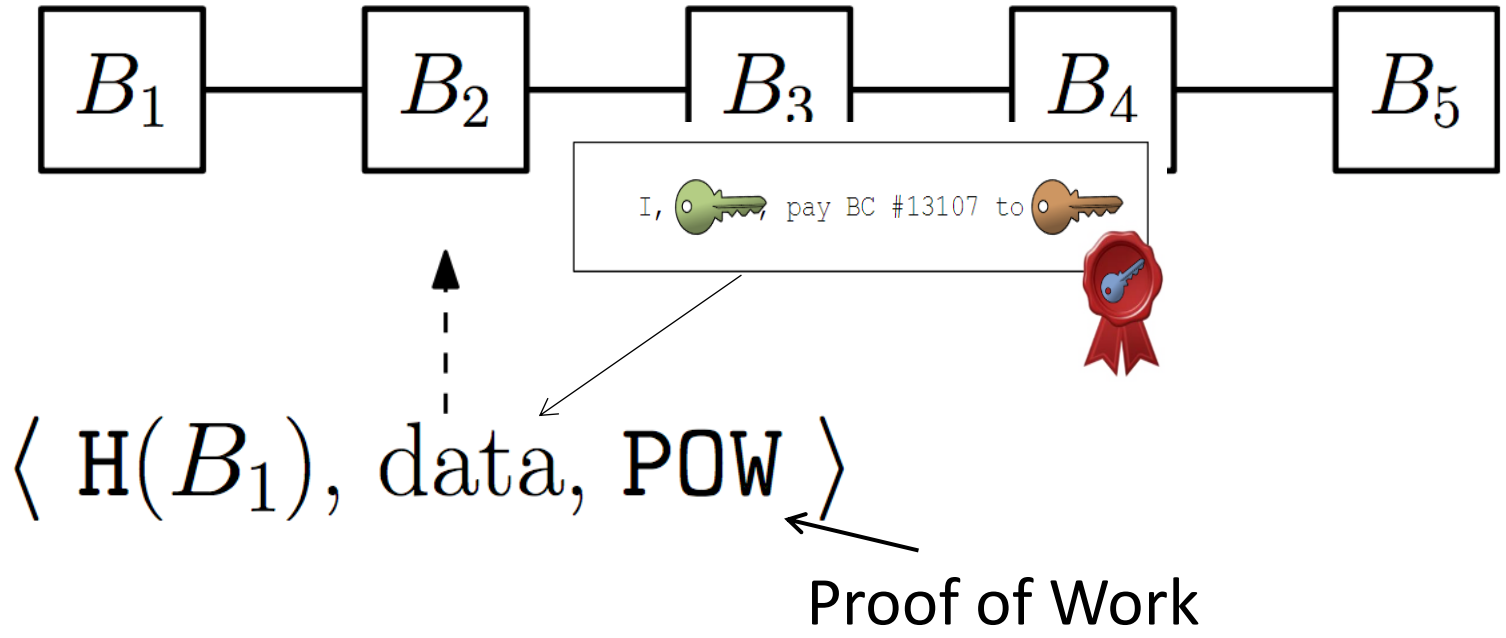
PoW-based Blockchain Protocols (Bitcoin)

- Parties (“miners”) have to do work in order to install a transaction
- Transactions are organized in chains of blocks



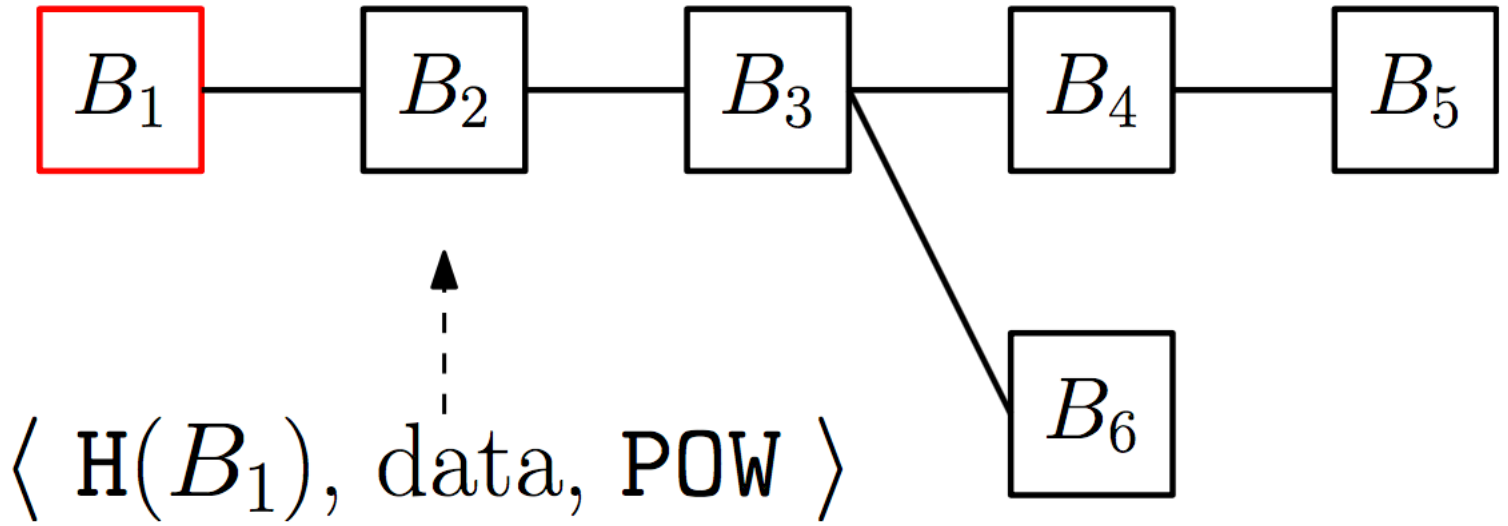
PoW-based Blockchain Protocols (Bitcoin)

- Parties ("miners") have to do work in order to install a transaction
- Transactions are organized in chains of blocks



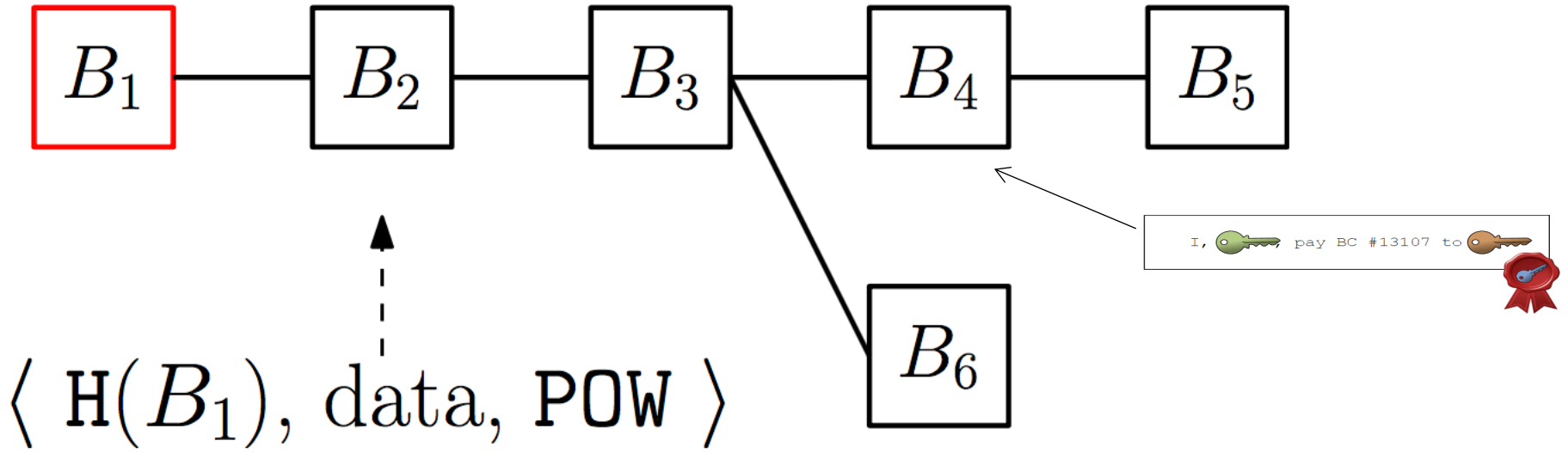
PoW-based Blockchain Protocols (Bitcoin) (2)

- Parties ("miners") always choose the *longest* chain they received



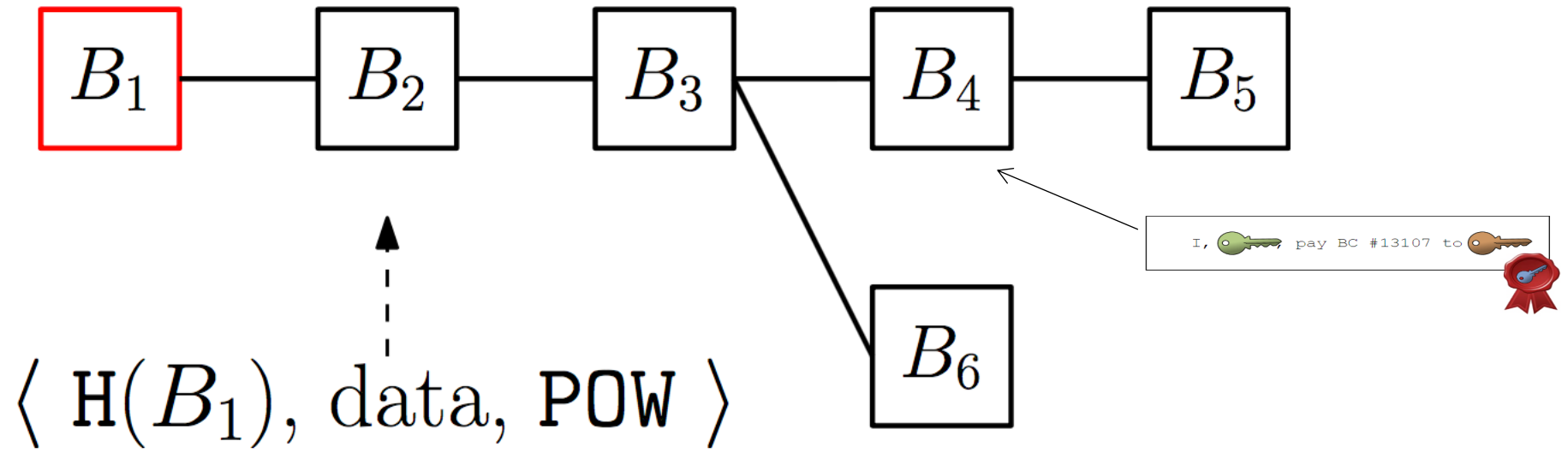
PoW-based Blockchain Protocols (Bitcoin) (3)

- Parties ("miners") always choose the *longest* chain they received
- If party wants to **erase** a transaction, it has to find a longer chain!



PoW-based Blockchain Protocols (Bitcoin) (4)

- Parties ("miners") always choose the *longest* chain they received
- If party wants to **erase** it transaction, it has to find a longer chain!



- If transaction is "sufficiently deep," it cannot do this unless it has a "majority of hashing power"!

The Intriguing “Permissionless” Model

The “Permissionless” Model [Nak08]

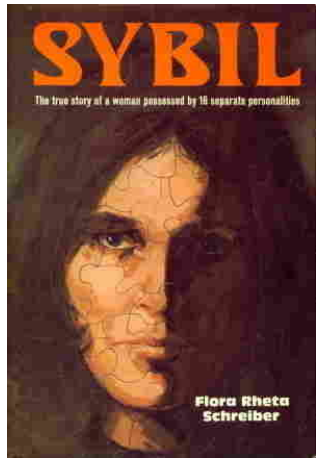
- Not a traditional distributed system
  - Nodes known *a priori* and authenticated

- The “permissionless” model
  - Nodes do *not* know each other (not even their exact number!)
  - Nodes come and go
  - *Anyone* can join

- And yet, realize a distributed ledger!

The "Permissionless" Model [Nak08] (2)

- Strong impossibility results w/o authentication [Oku05, BCLPR05]
- *Sybil* attacks are unavoidable [Dou02,…]
- ⅓ barrier in no. of misbehaving parties [LSP82, Bor96, Fit03]

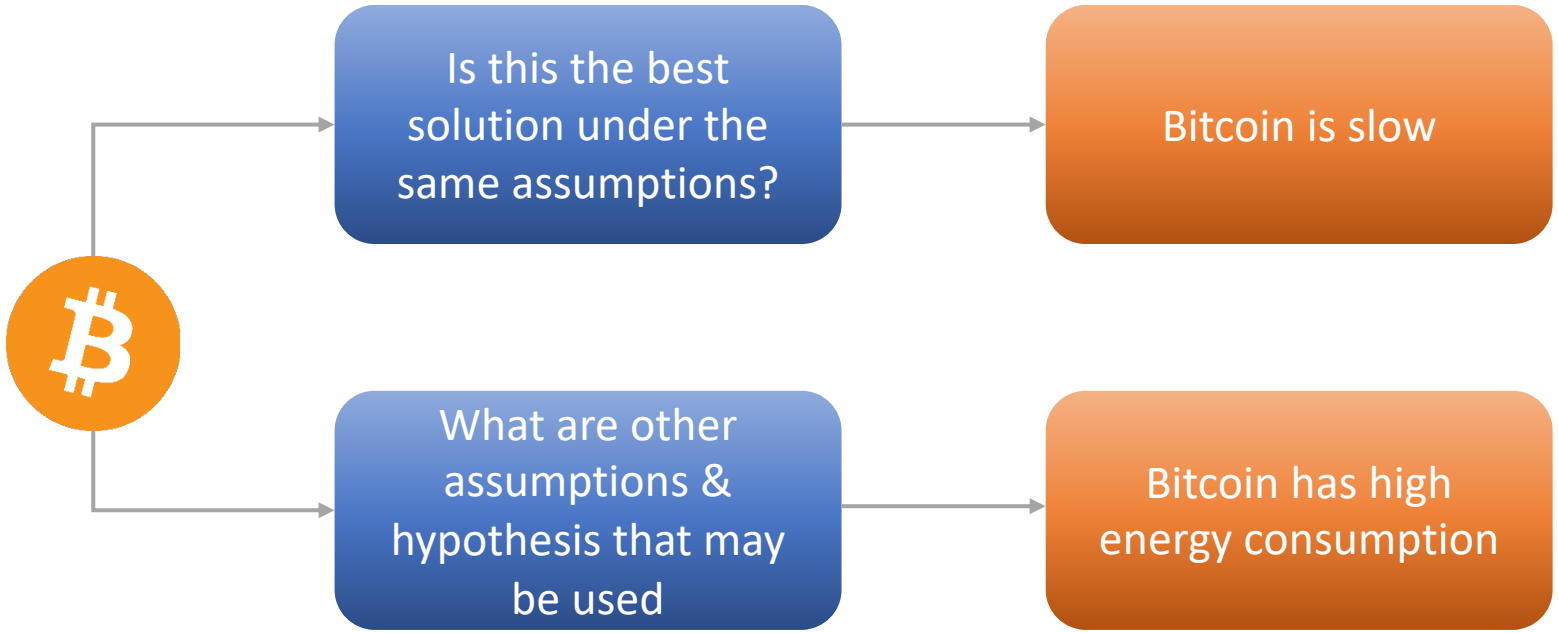


(Informal) Answer [Nak08]:

- The "*blockchain,*" based on Proofs of Work
- **Claim:** The blockchain realizes a "public ledger," assuming an *honest majority*
  - Consistency: Everyone sees the same history
  - Liveness: Everyone can add new transactions

Proofs of Stake

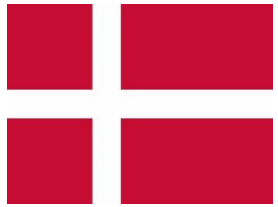
Bitcoin Challenges



~ 2000 tx/s

~ 100 tx/s

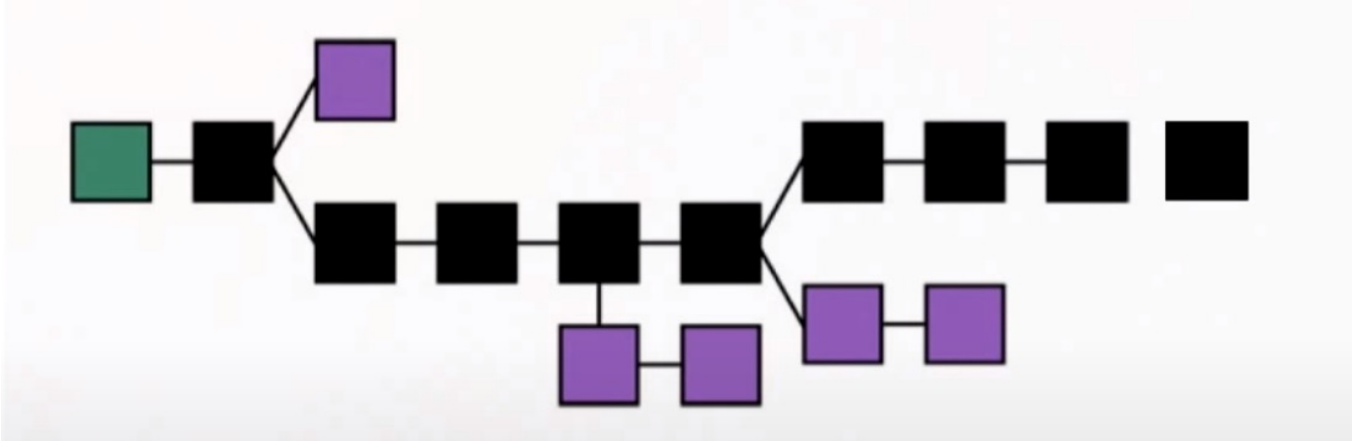
~ 15 tx/s



In 2020

Proof-of-Stake Background

- Generating the next block in Bitcoin is like an election



- A miner is elected with probability proportional to its hashing power
- "Collisions" may occur but they can be solved by the longest chain rule or a similar concept

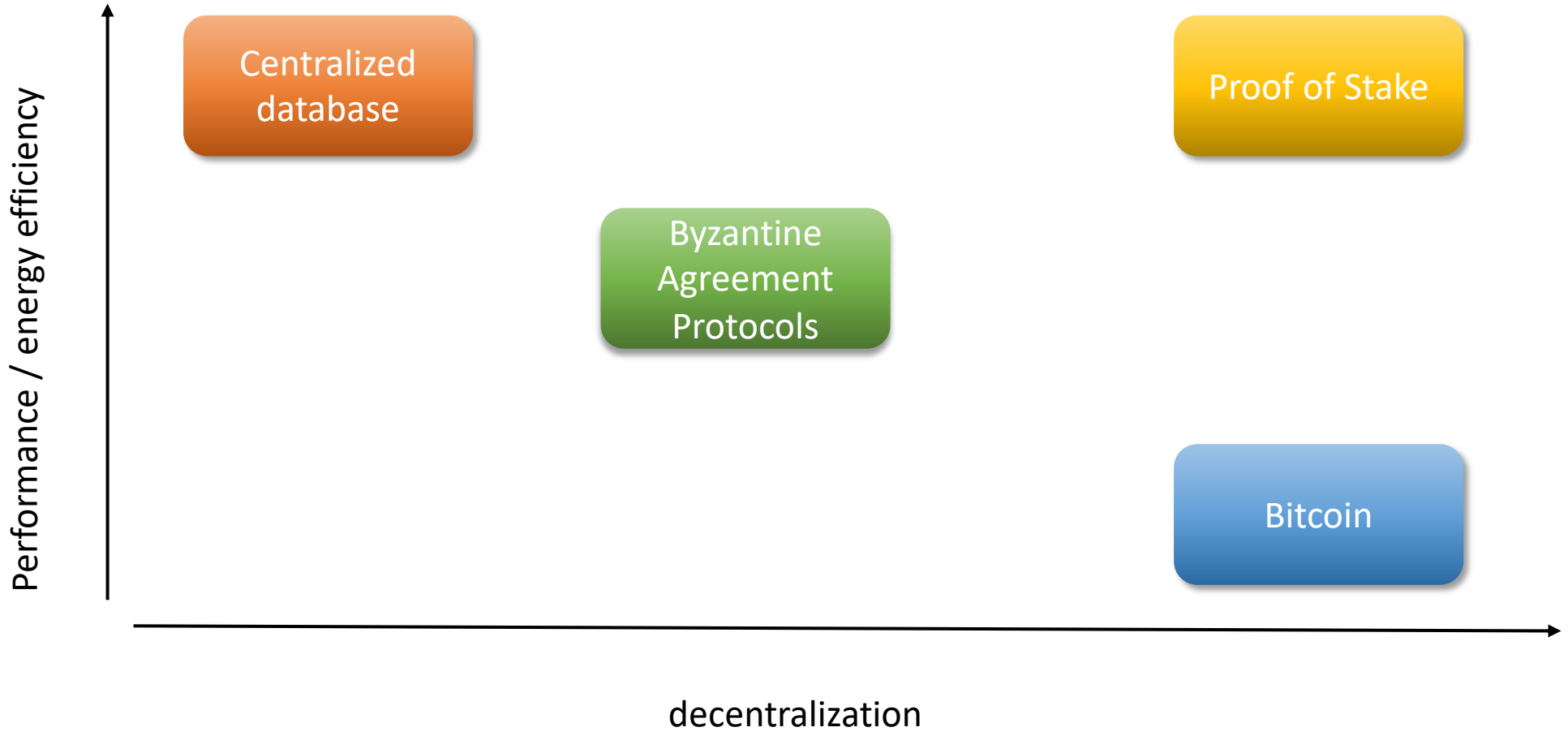
Proof of Stake

- Use stake (a ***virtual*** resource) instead of hashing power (a **physical** resource)

CARDANO

Algorand

Performance vs Decentralization



Proof-of-Stake Approaches

- PoS blockchains. Employ hash chains, digital signatures and some form of longest chain rule
  - E.g., Ouroboros, Snow White, Nxt
- PoS BFT. Adapt classical Byzantine fault-tolerant protocols to operate in the PoS setting
  - E.g., Algorand
- Both approaches are classified as PoS since protocol participation is based on the "proof of stake" primitive
- Fundamental enabling tool: ***Verifiable Random Functions*** (VRFs)

Verifiable Random Functions (VRFs) [MRS99]

- Cryptographic primitive that maps inputs to *verifiable* pseudorandom outputs
  - I.e., once a key pair (public key, secret key) and an input *X* are fixed, a VRF produces a unique pseudorandom **verifiable** output
- VRFs are the public-key version of a *keyed* cryptographic hash
  - Only the holder of the private key can compute the hash, but anyone with public key can verify the correctness of the hash


Thank You

Program

Monday, May 1st		
10:00 AM - 10:30 AM	Coffee	
10:30AM - 11:00 AM	Juan Garay, Texas A&M	Welcome & Blockchain Warm Up
11:00 AM - 11:30 PM	Le Xie, Texas A&M	Blockchain and Energy: Understanding the Impact of Cryptomining on the Electric Grid
11:30 PM - 12:00 PM	Korok Ray, Texas A&M	Banking in Bitcoin
12:00 PM - 1:15 PM	Lunch (provided)	
1:15 PM - 2:15 PM	Oshani Seneviratne, RPI	Empowering Decentralization through Algorand's Smart Contracts
2:15 PM - 2:30 PM	Ishan Dhanani, TAMU Blockchain Club	RevPass: Revolutionizing the Sports Passes
2:30 PM - 3:00 PM	Coffee Break	
3:00 PM - 4:00 PM	Tal Rabin, UPenn	YOSO: You Only Speak Once – Secure MPC with Stateless Ephemeral Roles