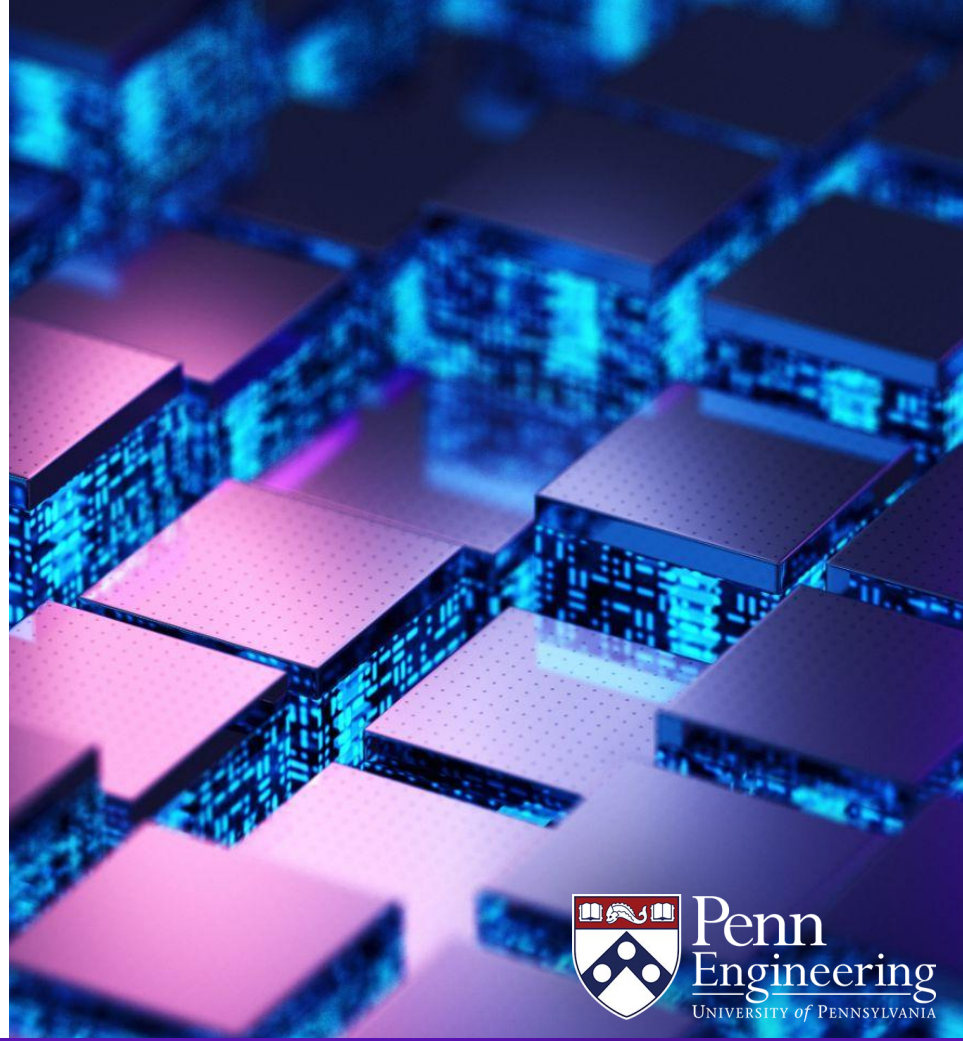
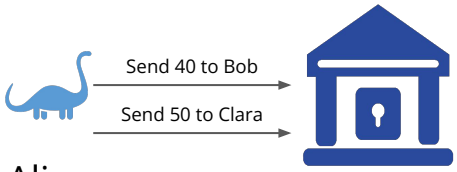
EAS 5830: BLOCKCHAINS

Basics of Blockchain Design

Professor Brett Hemenway Falk



Blockchains are about ordering



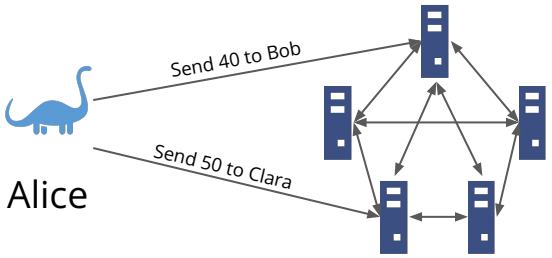
Bob

Clara

Ledger authenticates request(s) came from Alice
Which one is “valid”?

User	**Balance**
Alice	80
Bob	100
Clara	200

Blockchains are about ordering



Bob

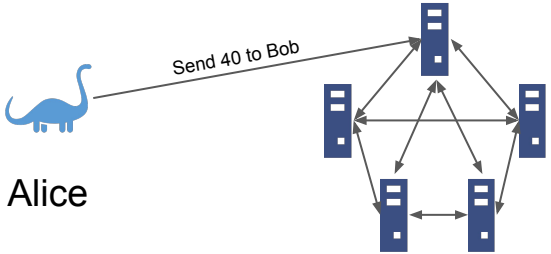
Clara

Ordering is much more challenging in the distributed setting

User	**Balance**
Alice	80
Bob	100
Clara	200

How are transactions ordered?

1. Alice sends a “transaction” to any one of the nodes (aka “miners” or “validators”)
2. Nodes gossip transactions among themselves
3. One node is selected to produce a “block”
   a. Selection process varies by blockchain
4. Block producer has complete autonomy to order transactions
5. Block producer circulates block to other nodes
6. Nodes “validate” block
   a. Validation process varies by chain
7. Blockchain data structure ensures blocks aren’t reordered



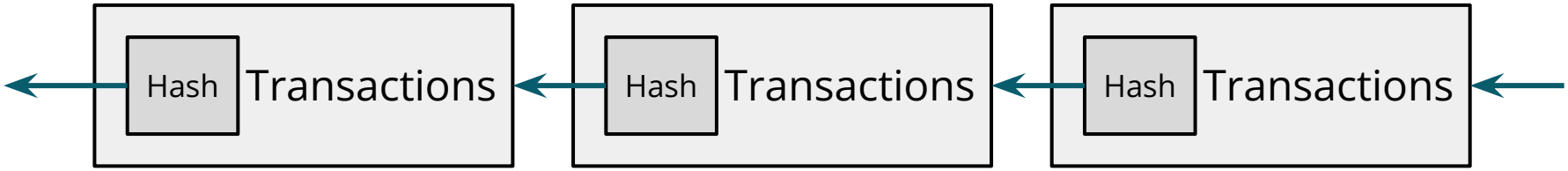
How are transactions ordered?

1. Alice sends a “transaction” to any one of the nodes (aka “miners” or “validators”)
2. Nodes gossip transactions among themselves
3. One node is selected to produce a “block”
    a. Selection process varies by blockchain
4. Block producer has complete autonomy to order transactions
5. Block producer circulates block to other nodes
6. Nodes “validate” block
    a. Validation process varies by chain
7. Blockchain data structure ensures blocks aren’t reordered

Blockchain cryptography

- Hash functions
  - Create a digital “fingerprint”
  - Detects tampering
- Digital signatures
  - Verify the provenance of a message

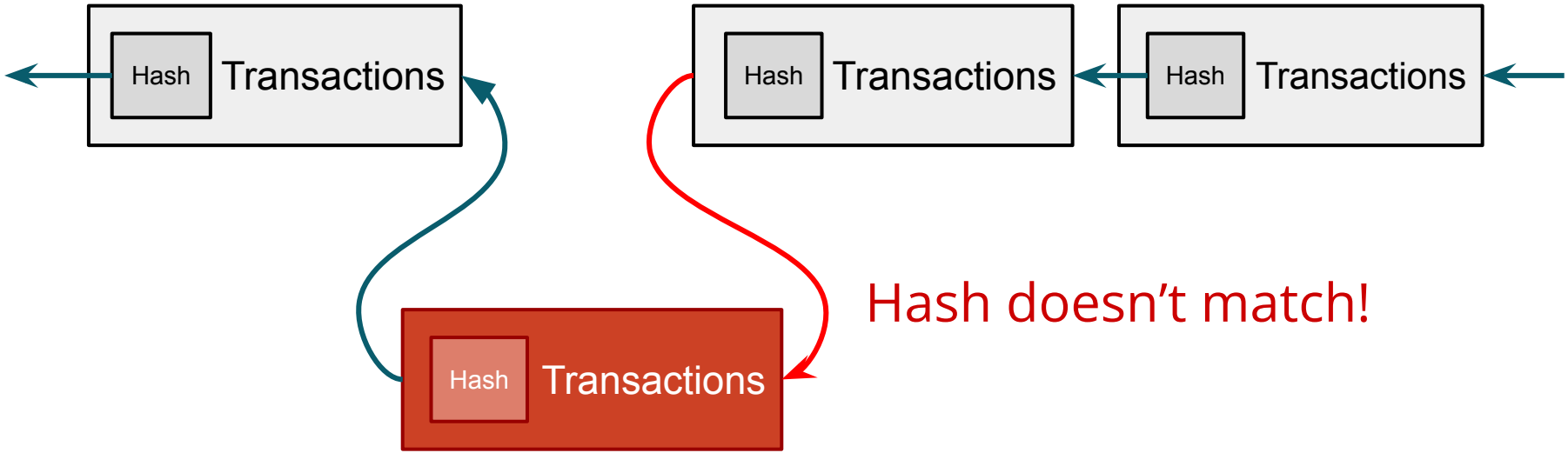
The blockchain data structure



- Transactions (updates) are application dependent
  - Payments
  - Messages
  - Unstructured data
- Each block has the “hash” of the previous block
- The cryptographic hash ties each block to its predecessor

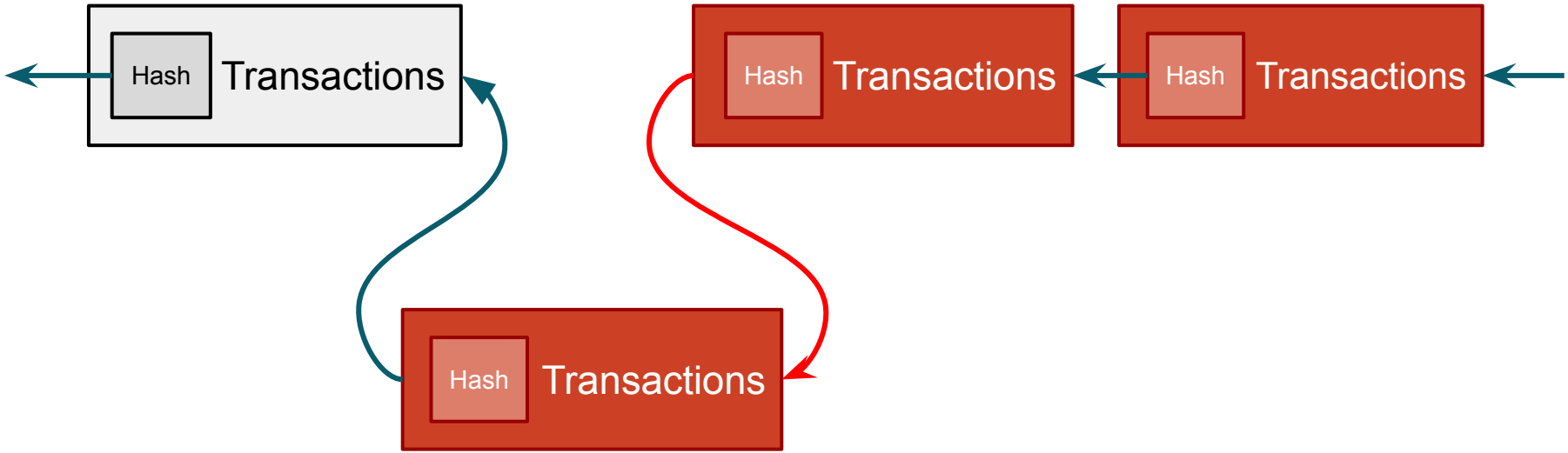
The blockchain data structure

- Tampering with the content of any block can easily be detected.

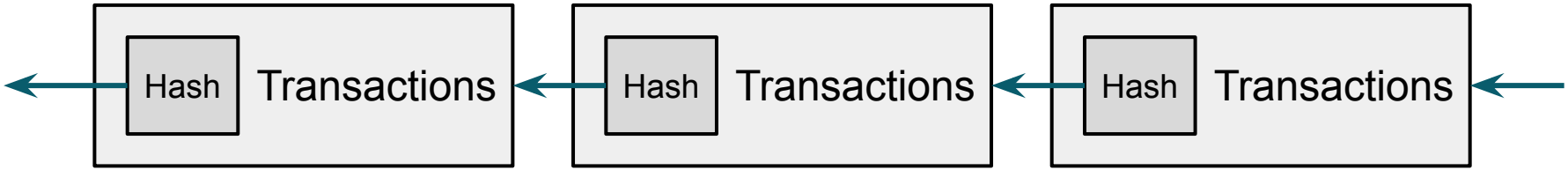


The blockchain data structure

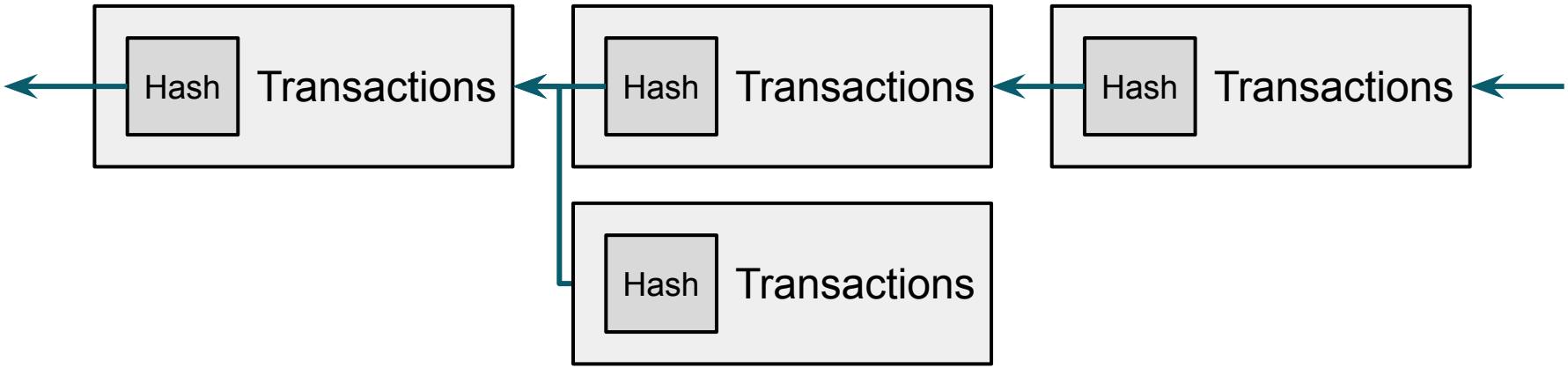
- If you want to change one block, you must change all the blocks that follow it
- This makes the blockchain an append-only data structure



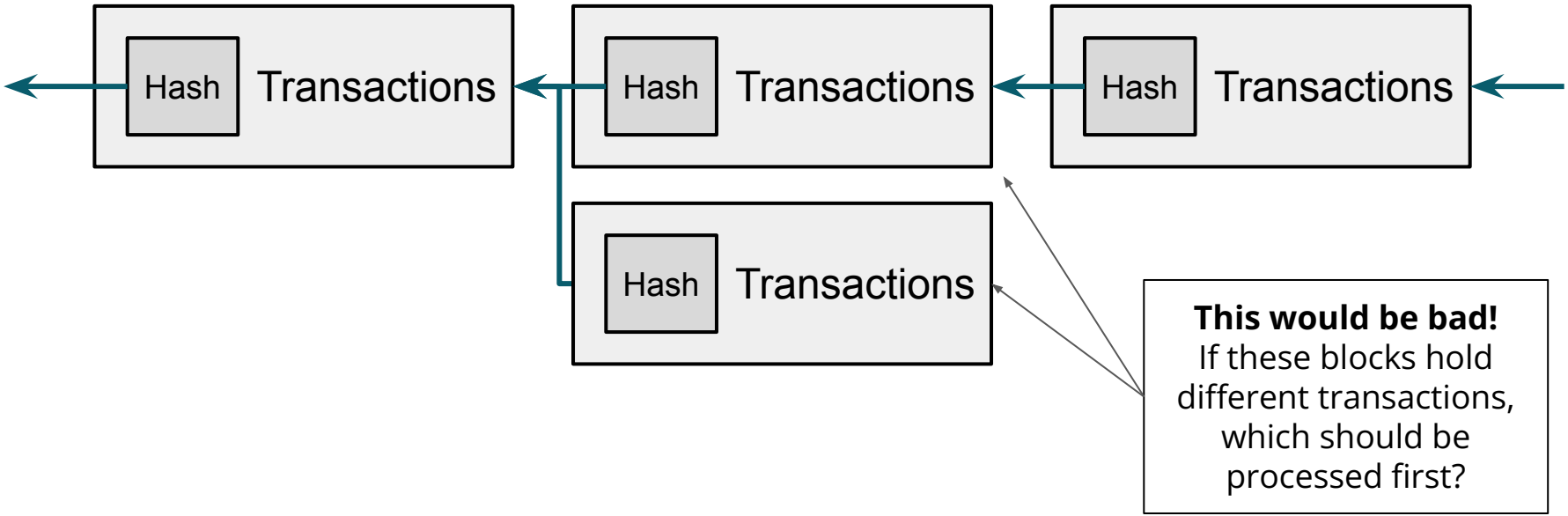
Appending to the “end”



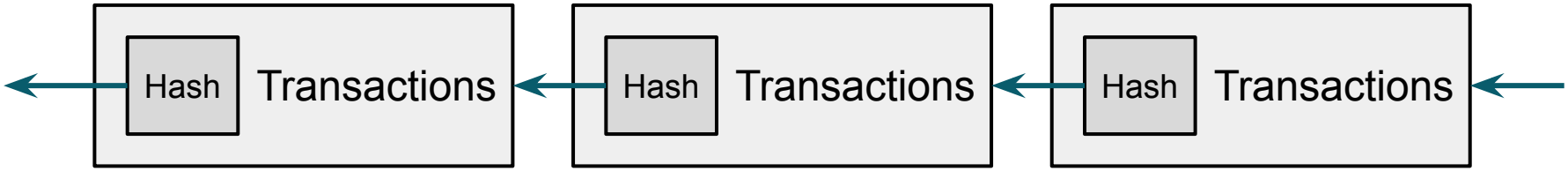
Appending to the “end”



Appending to the “end”



Blockchains in the distributed setting



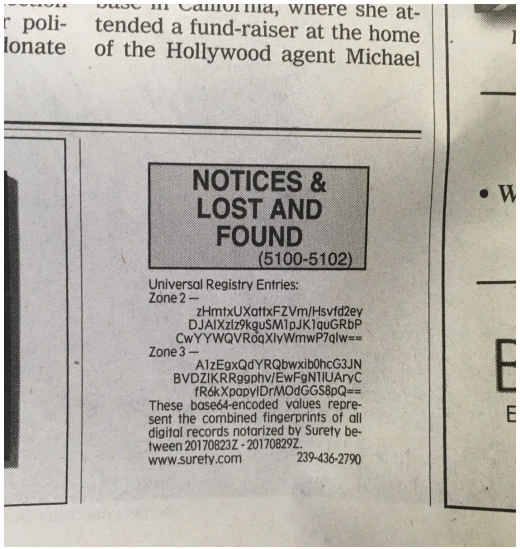
- Each node in the network maintains a copy of the blockchain
- If we can agree on the first and last block of a chain, then the hashes ensure that we agree on the entire chain

Consensus (agreeing on the last block)

- Permissioned: (“one entity one vote”)
  - Pro: Efficient
  - Con: Validators need to be known and trusted
- Proof-of-work: (“one CPU one vote”)
  - Pro: No restrictions on the validators
  - Con: Slow, wasteful, energy-intensive
    - Bitcoin can only handle a few transactions per second
    - Bitcoin validators use a huge amount of electricity
- Proof-of-stake: (“one dollar one vote”)
  - Pro: Efficient
  - Con: Leads to centralization?

Hash Chains in the New York Times

- Users submit record to Surety
- Surety signs record
- Surety gathers records into a block
- Surety posts hash of new block + previous block and posts hash to NYT



Summary

- Keeping track of a database requires
  - Checking identity of sender (Digital signatures)
  - Agreeing on the order of transactions