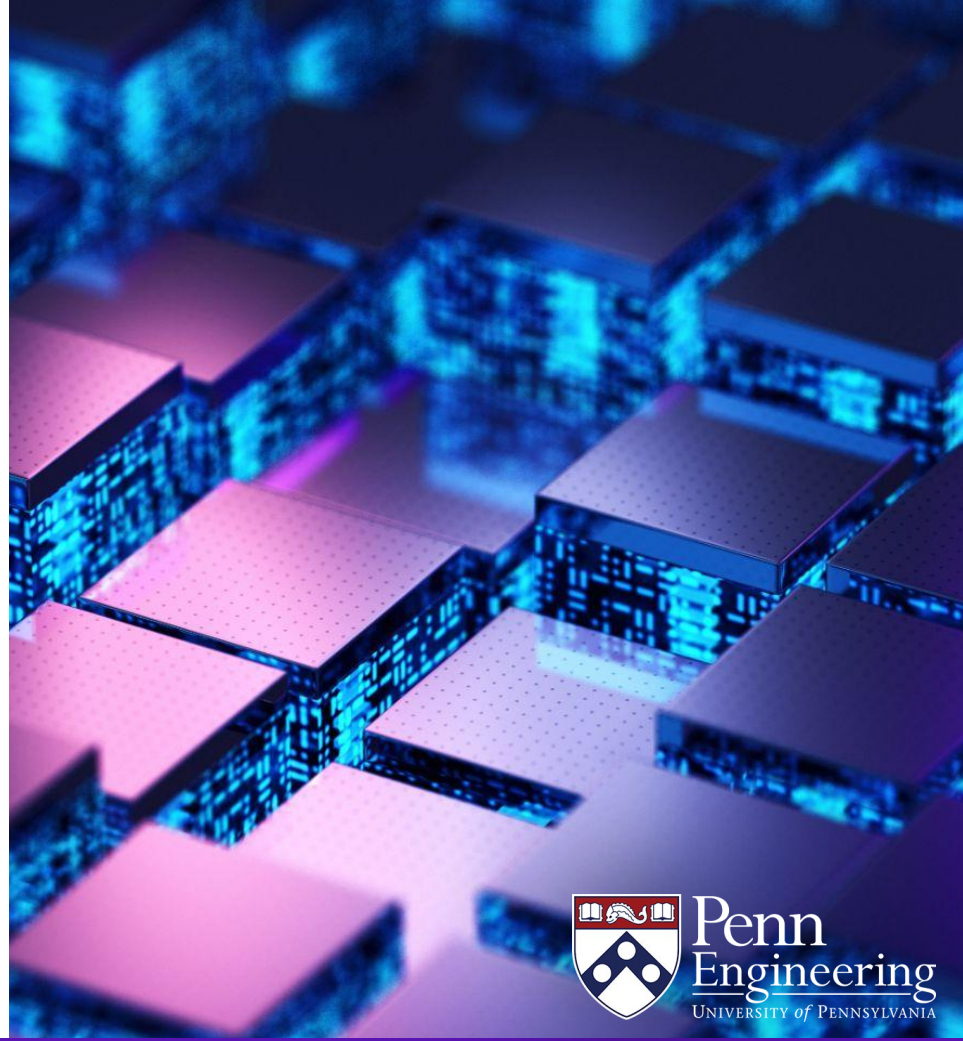
EAS 5830: BLOCKCHAINS

Hash Chains

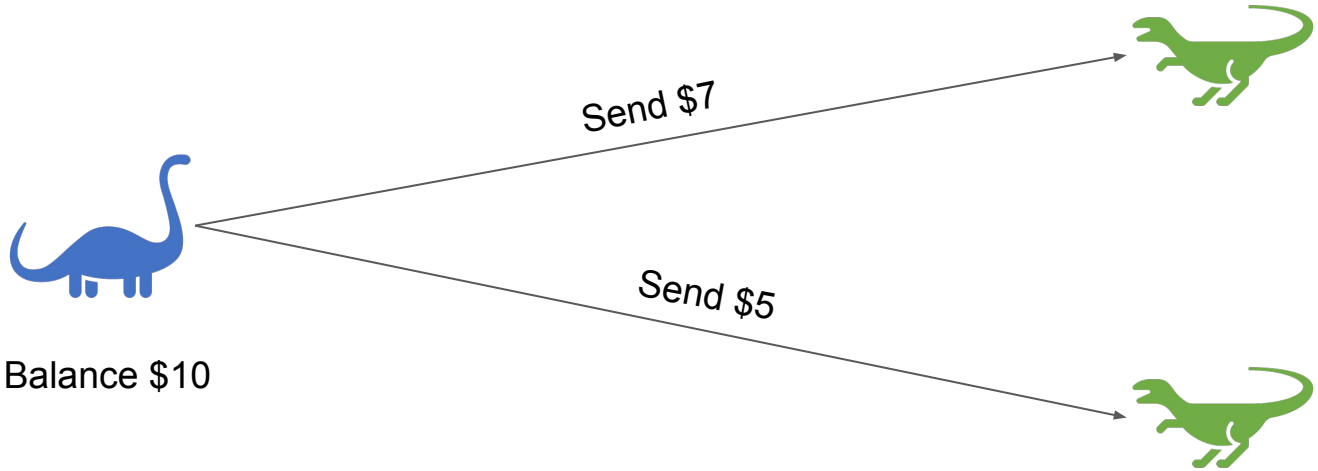
Dr. Brett Hemenway Falk



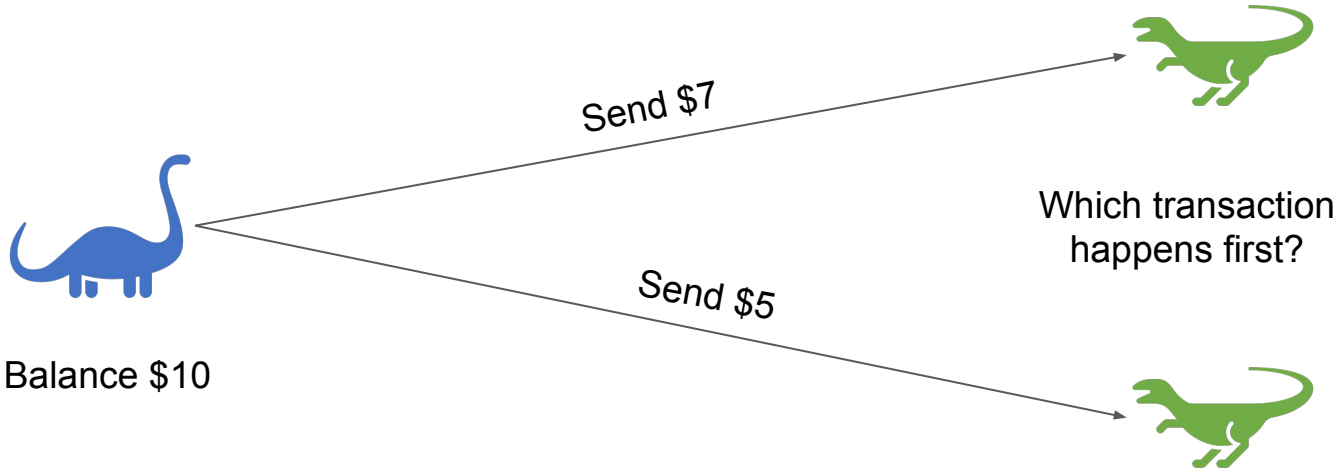
Learning goals

- Hash chains
  - An append-only data structure
- Applications of hash chains

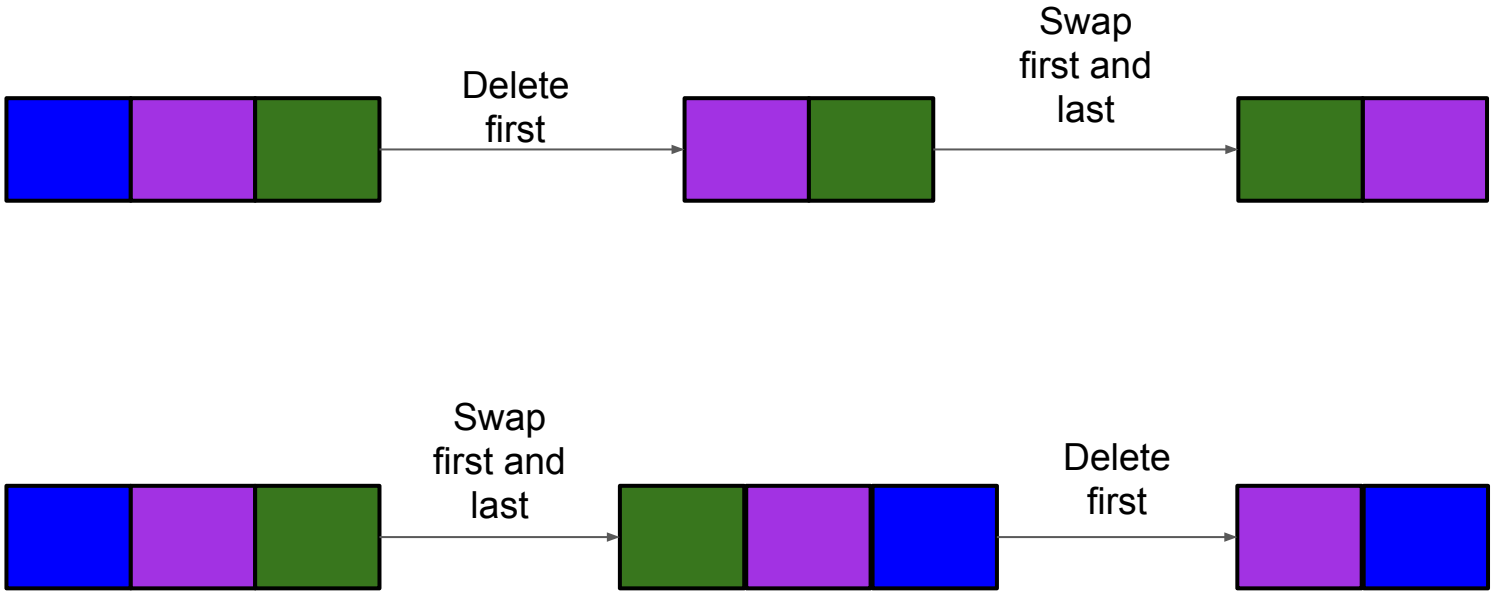
Ordering transactions



Ordering transactions

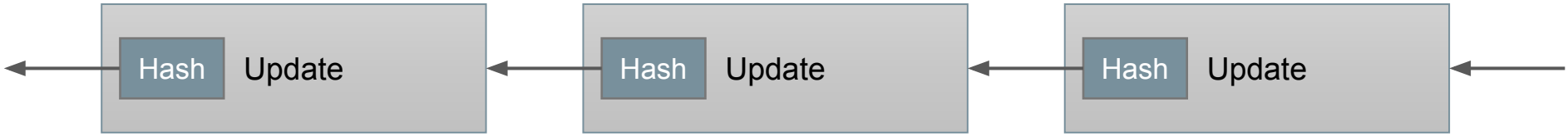


Ordering updates

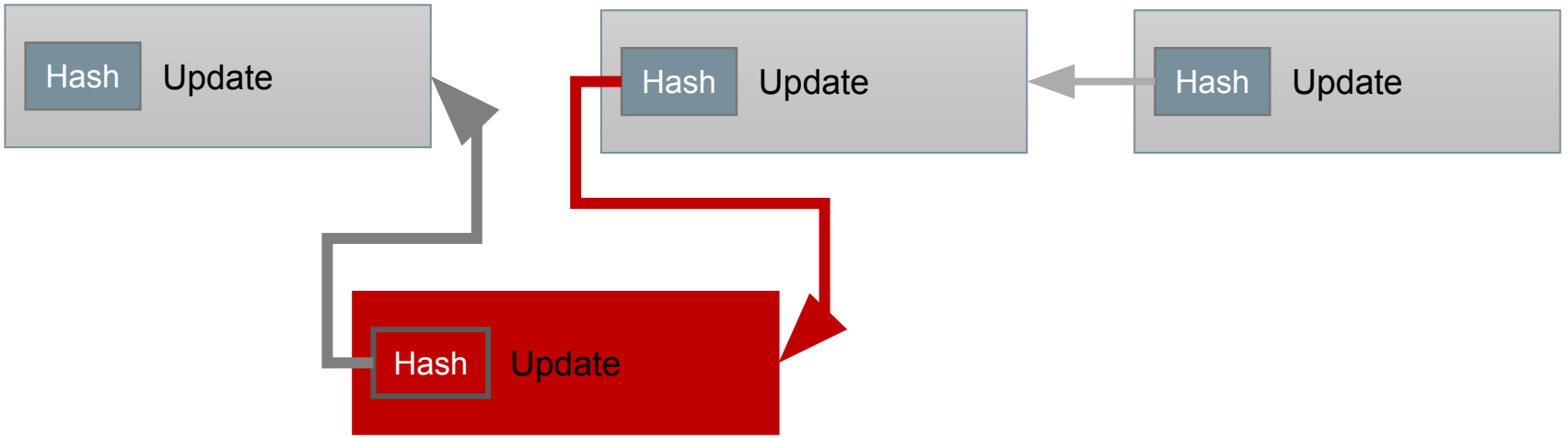


Hash chains

- Chain of “blocks”
- Each block contains data
  - e.g. transactions
- Each block contains a hash of its predecessor
- Collision resistance means that each block determines all its predecessors

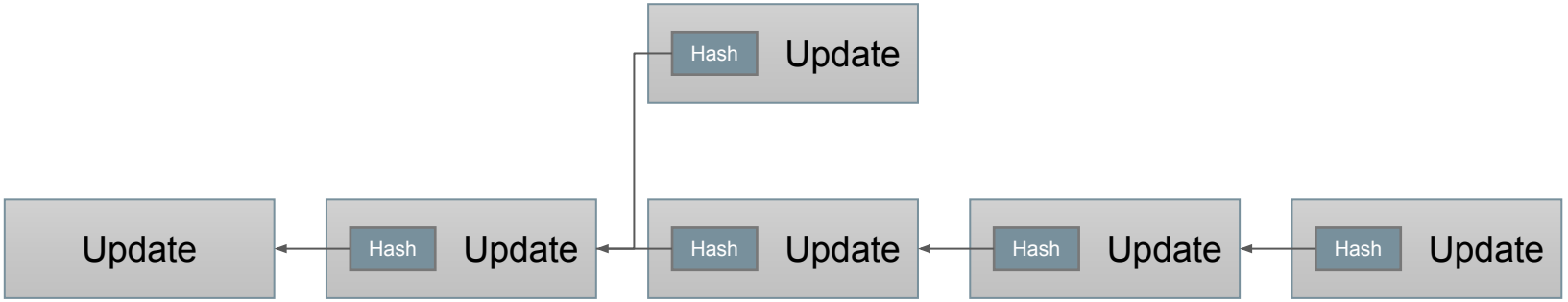


Hash chains prevent insertions



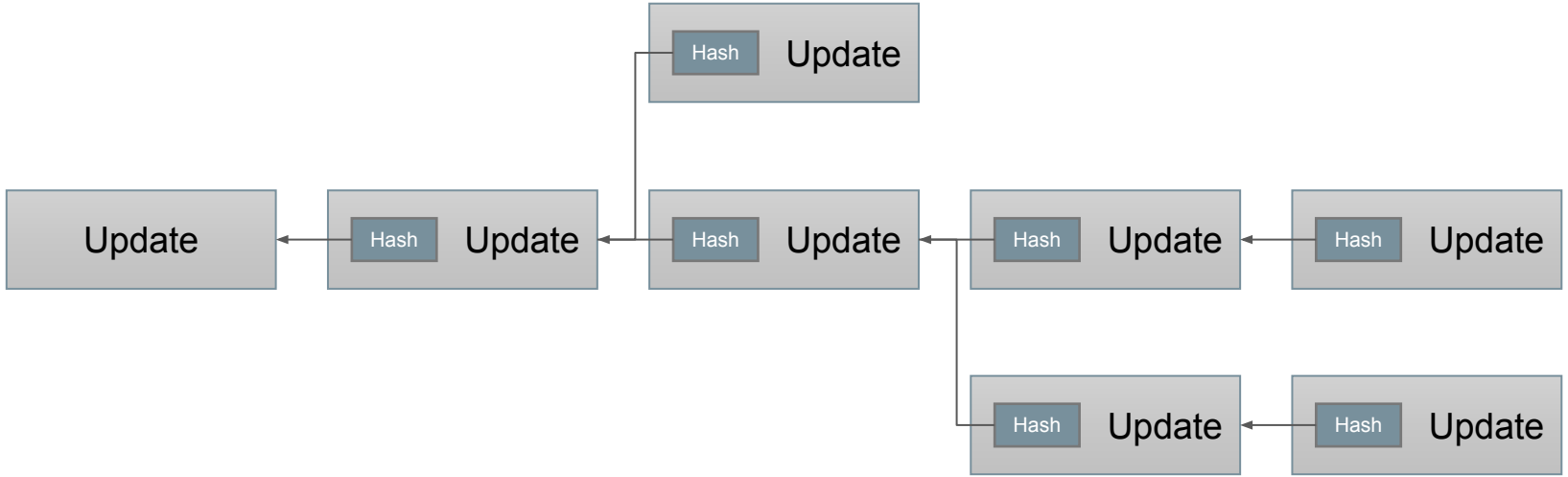
Appending is easy

- There's no well-defined notion of the "end" of the chain
- You can append onto any block



Appending is easy

- There's no well-defined notion of the "end" of the chain
- You can append onto any block



Hash chains simplify consensus

If we can agree on the first block and the last block of the chain, then we agree on the whole chain

Hash chains simplify consensus

If we can agree on the first block and the last block of the chain, then we agree on the whole chain

Easy to agree on first block - set it to 0

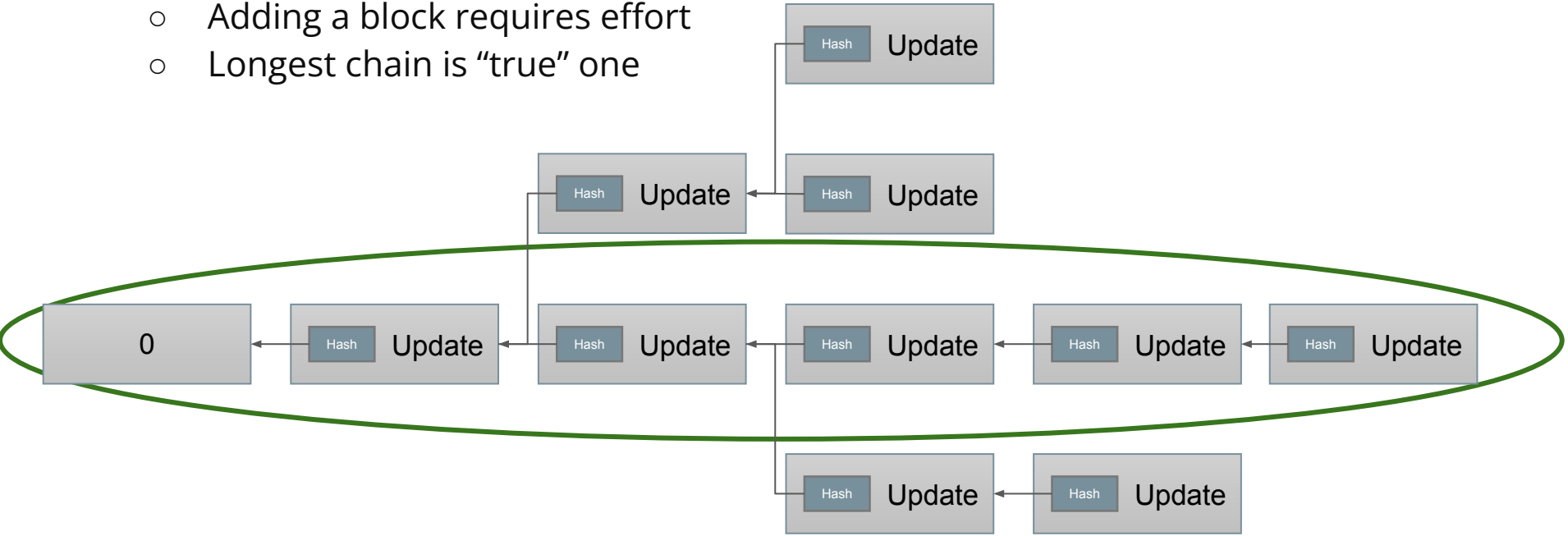
Hash chains simplify consensus

If we can agree on the first block and the last block of the chain, then we agree on the whole chain

How do you agree on last block?

Agreeing on last block

- Satoshi's idea
  - Adding a block requires effort
  - Longest chain is "true" one



Git

- There isn't always one "true" history
- Each node uniquely defines a state