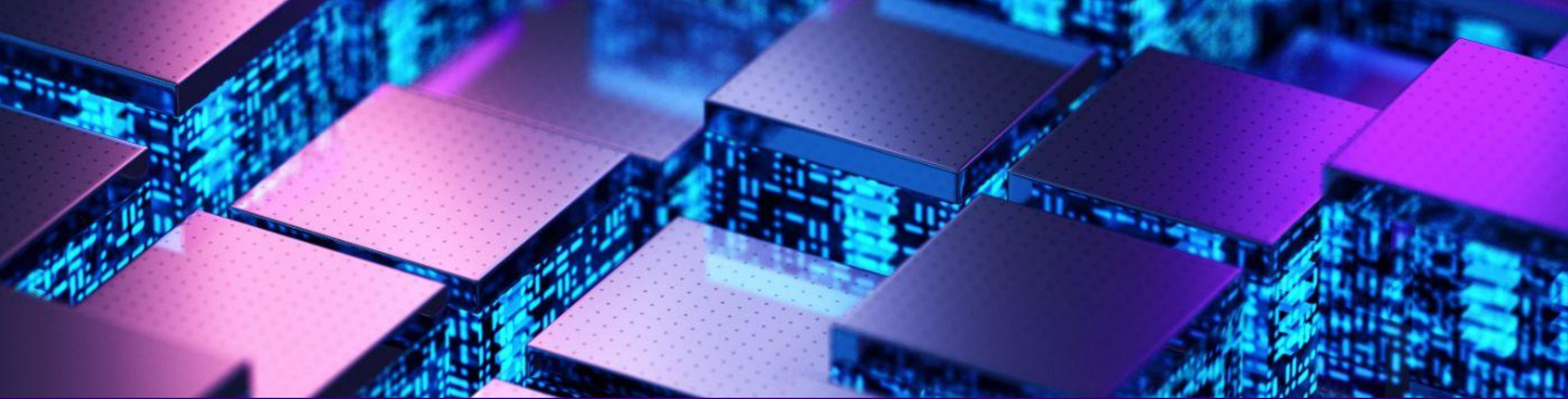


EAS 5830: BLOCKCHAINS

# Front-running Approvals

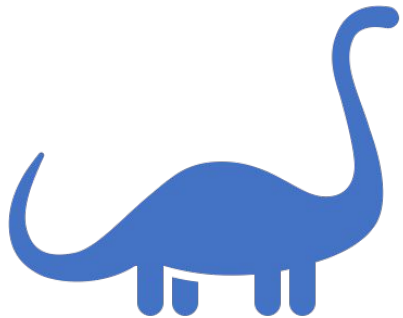
Professor Brett Hemenway Falk



# Approvals

# Approving transactions


approve(, 4)



Alice





**UPN**

Alice	10
Bob	12
Charlie	10
Deborah	11
	12





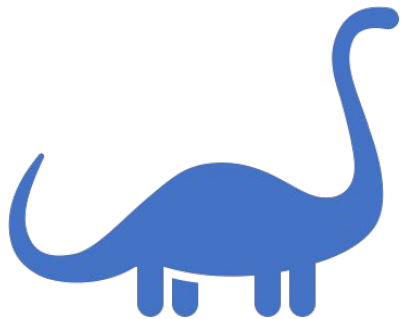
**Uniswap**

	12
	12

# Approving transactions



approve(, 4)

	<b>UPN</b>
Alice	10
Bob	12
Charlie	10
Deborah	11
	12



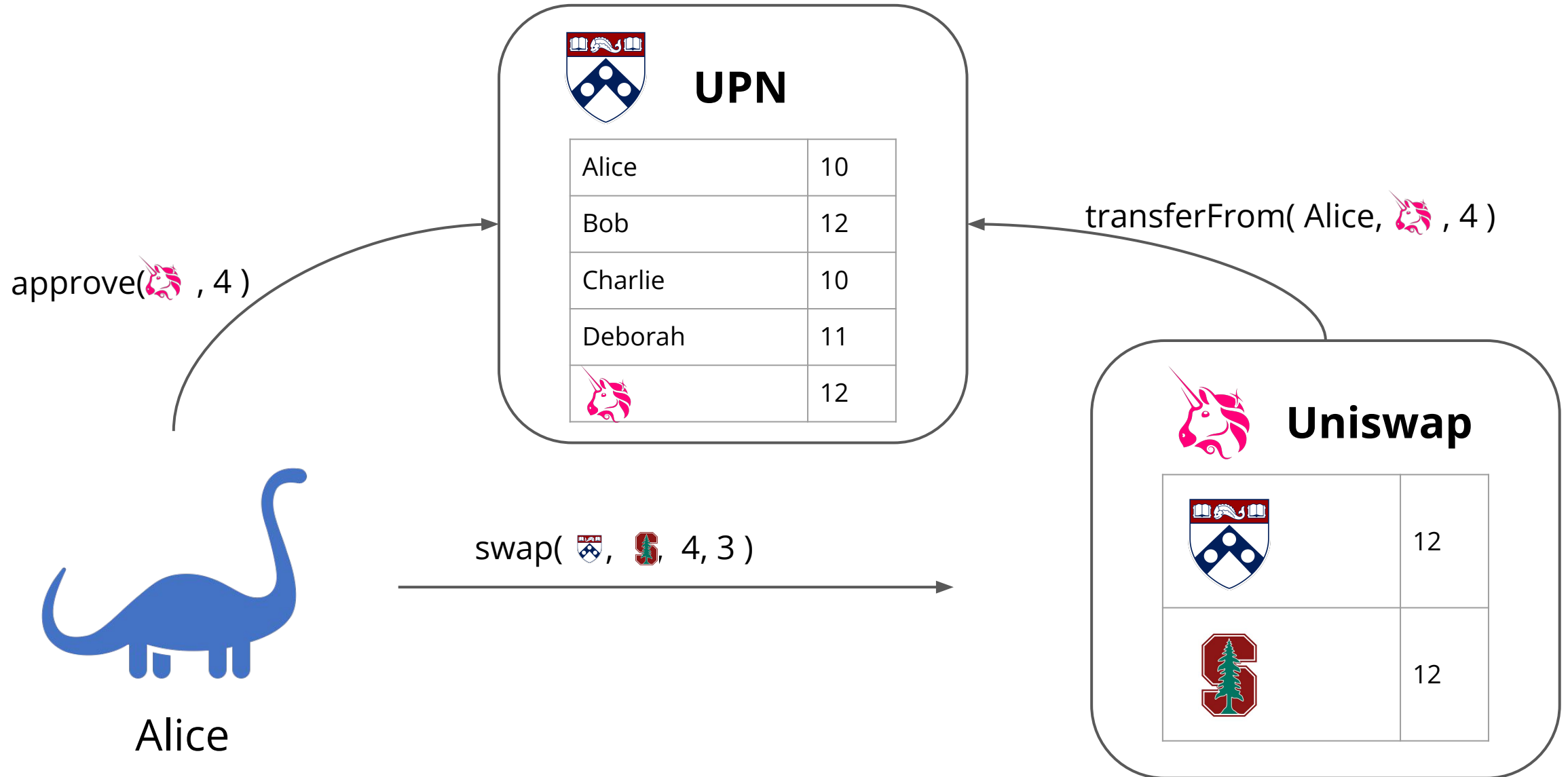
Alice

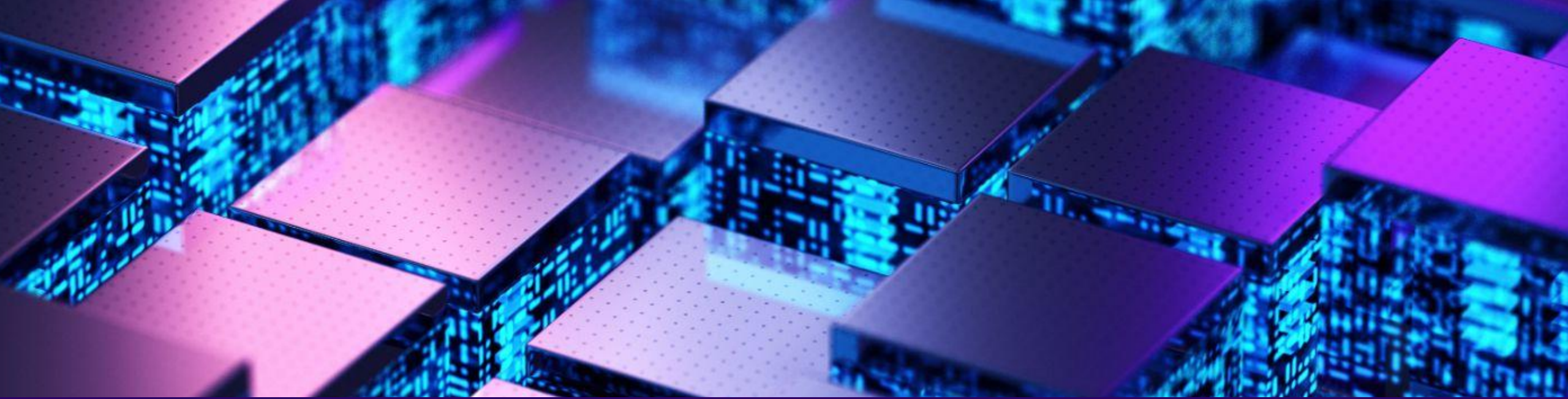
swap(, , 4, 3)

	<b>Uniswap</b>
	12
	12



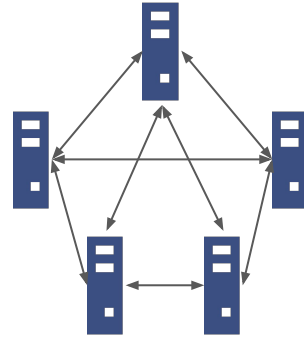
# Approving transactions





# The Approval Vulnerability

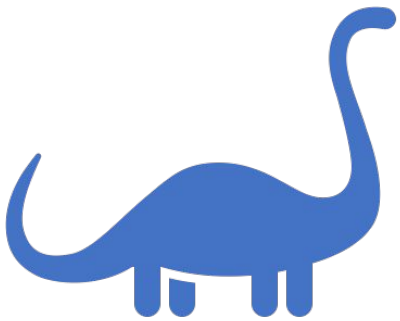
# Front-running approvals



**UPN**

Allowances

Alice	Bob: 100 Charlie: 20
Bob	Charlie: 5
Charlie	Deborah: 10

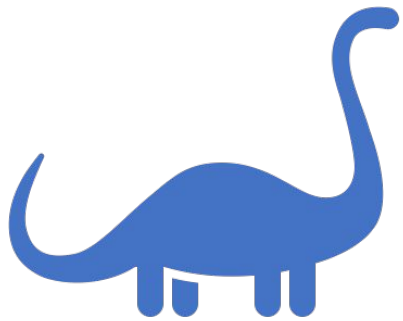
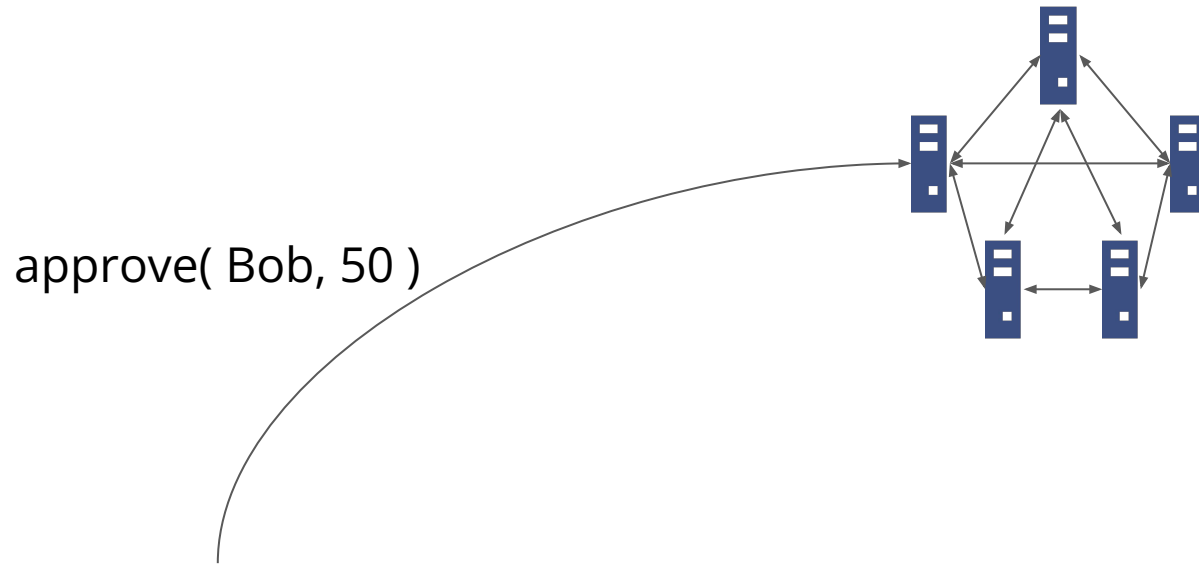


Alice



Bob

# Front-running approvals



Alice



Bob



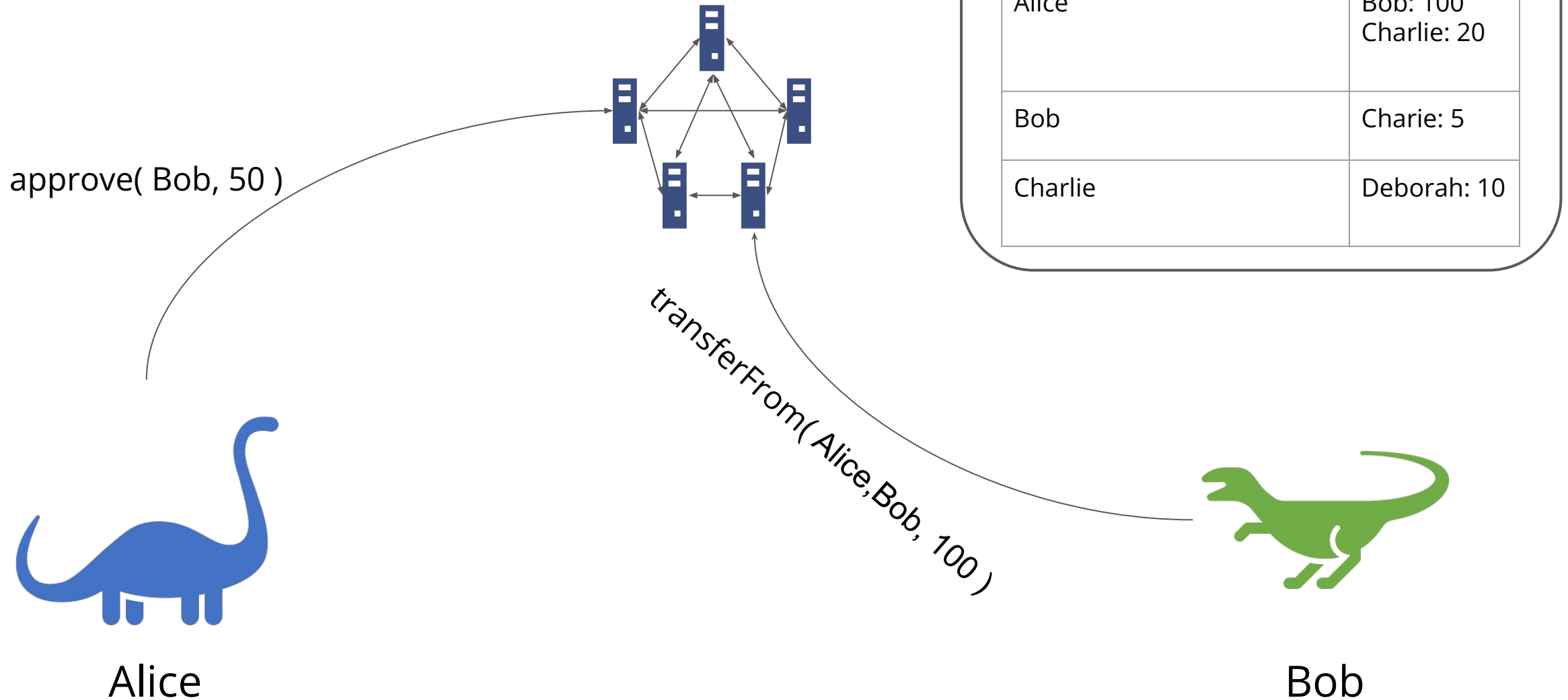
**UPN**

Allowances

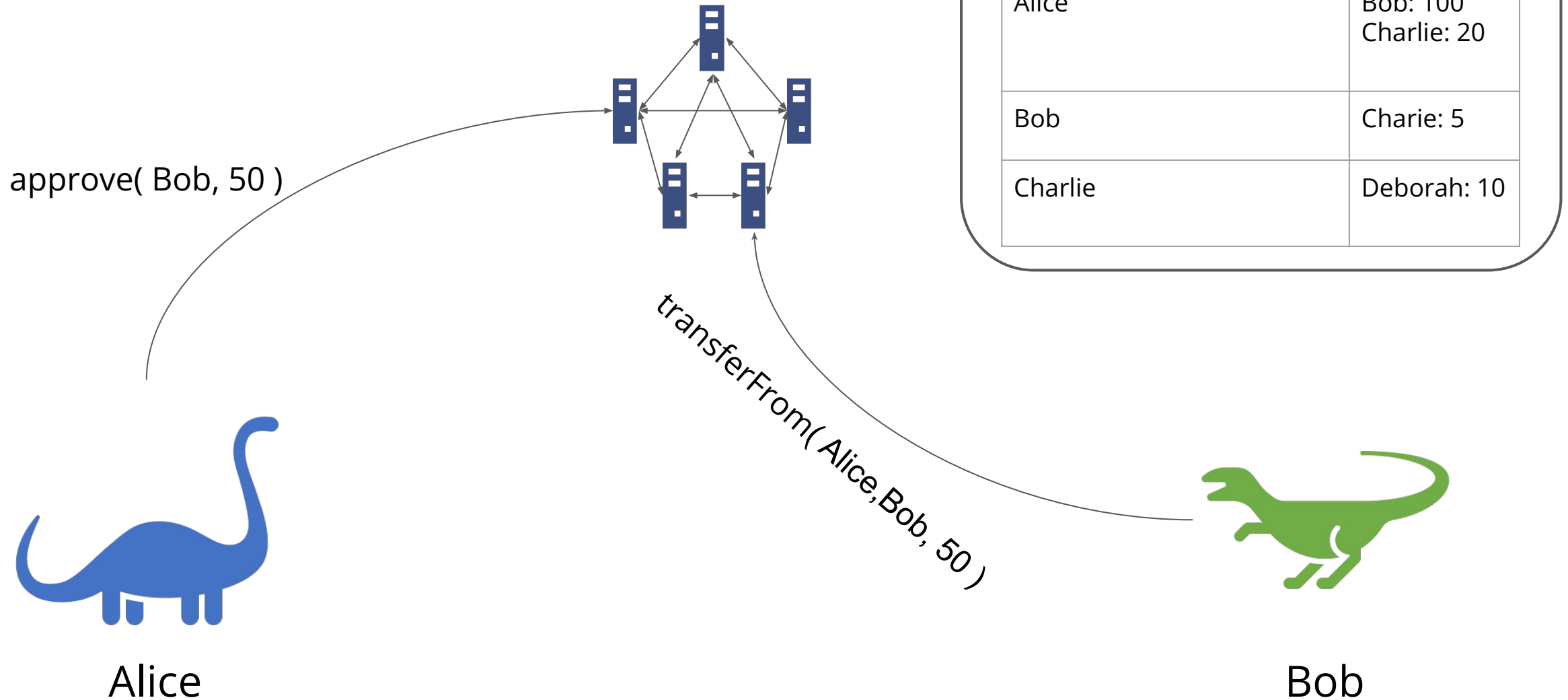
Alice	Bob: 100 Charlie: 20
Bob	Charlie: 5
Charlie	Deborah: 10



# Front-running approvals



# Front-running approvals



# Sandwiching approvals

## Temporal order

1. Alice sends  
approve(Bob,50)
2. Bob sends  
transferFrom(Alice,Bob,100)
3. Bob sends  
transferFrom(Alice,Bob,50)

## Blockchain order

1. transferFrom(Alice,Bob,100)
2. approve(Bob,50)
3. transferFrom(Alice,Bob,50)

# Mitigations

- When changing approvals, approve 0 first
  - approve(Bob,0) - wait for this transaction to be confirmed
  - approve(Bob,50)
- Some contracts implement
  - OpenZeppelin reference ERC20 has increaseAllowance, decreaseAllowance
  - USDC v2 implemented increaseAllowance and decreaseAllowance
  - PyUSD has increaseApproval, decreaseApproval



---

Copyright 2023 University of Pennsylvania  
No reproduction or distribution without permission.