



CMPSC 302

WEB DEVELOPMENT



# On Web3, we wear masks



Logo for Metamask, a crypto “wallet”

Head to [metamask.io](https://metamask.io) to download and add to your browser (preferably Chrome/Firefox; something that can handle plugins)



## And we live on different “nets”

- \* We'll set our active “network” (i.e. universe) to the Rinkelby TestNet
- \* Here, I'll be able to give you the crypto equivalent of fake Ethereum (a currency)
- \* Once you've completed this, head to the spreadsheet in the Discord channel to record your wallet number



# Drips and drabs

- \* I'll send you .004 (or so) of a single token
  - \* That's way more than we'll need to play our game
- \* We'll have a look at how this resolves together
- \* In the meantime, have a look at our assignment repository
  - \* It's in the Discord now





# The Social Contract

- ✦ Web3 is decentralized and it needs to be governed by “contracts”
- ✦ These contracts live in the cloud, and (for this activity), ours is simple:
  - ✦ We can:
    - ✦ Get the latest status
    - ✦ Set the latest status





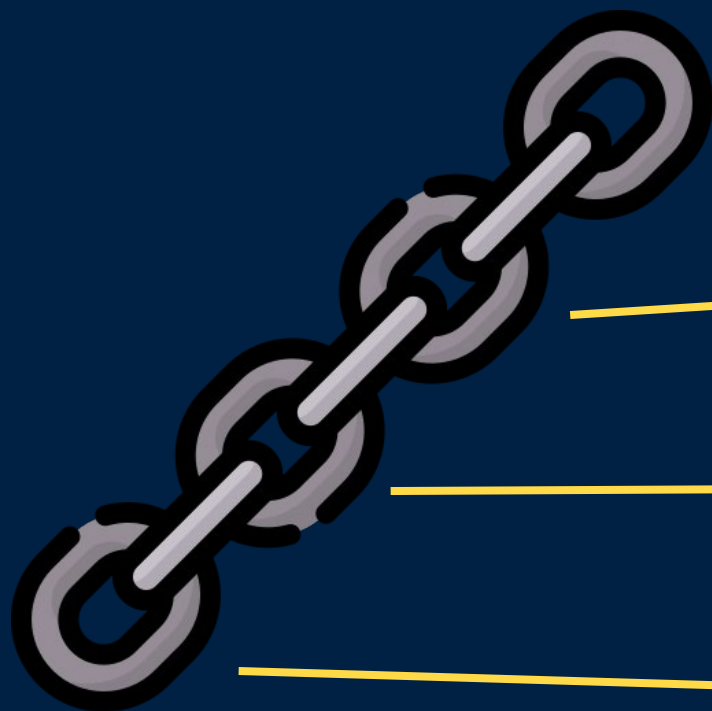
# The Social Contract

- ✦ Web3 is decentralized and it needs to be governed by “contracts”
- ✦ These contracts live in the cloud, and (for this activity), ours is simple:
  - ✦ We can:
    - ✦ Get the latest status
    - ✦ Set the latest status

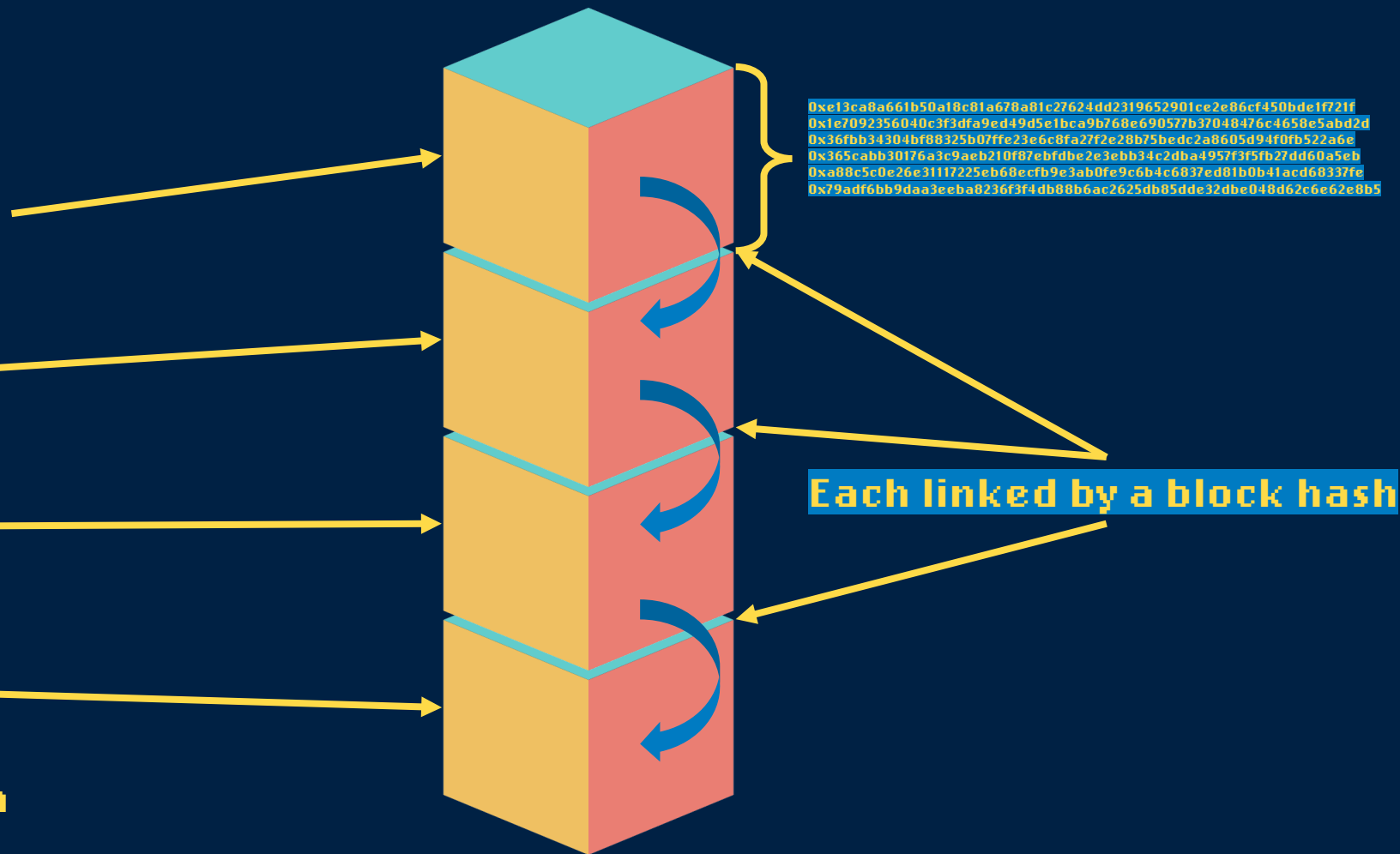




# wtf is blockchain



Actual photo of a blockchain





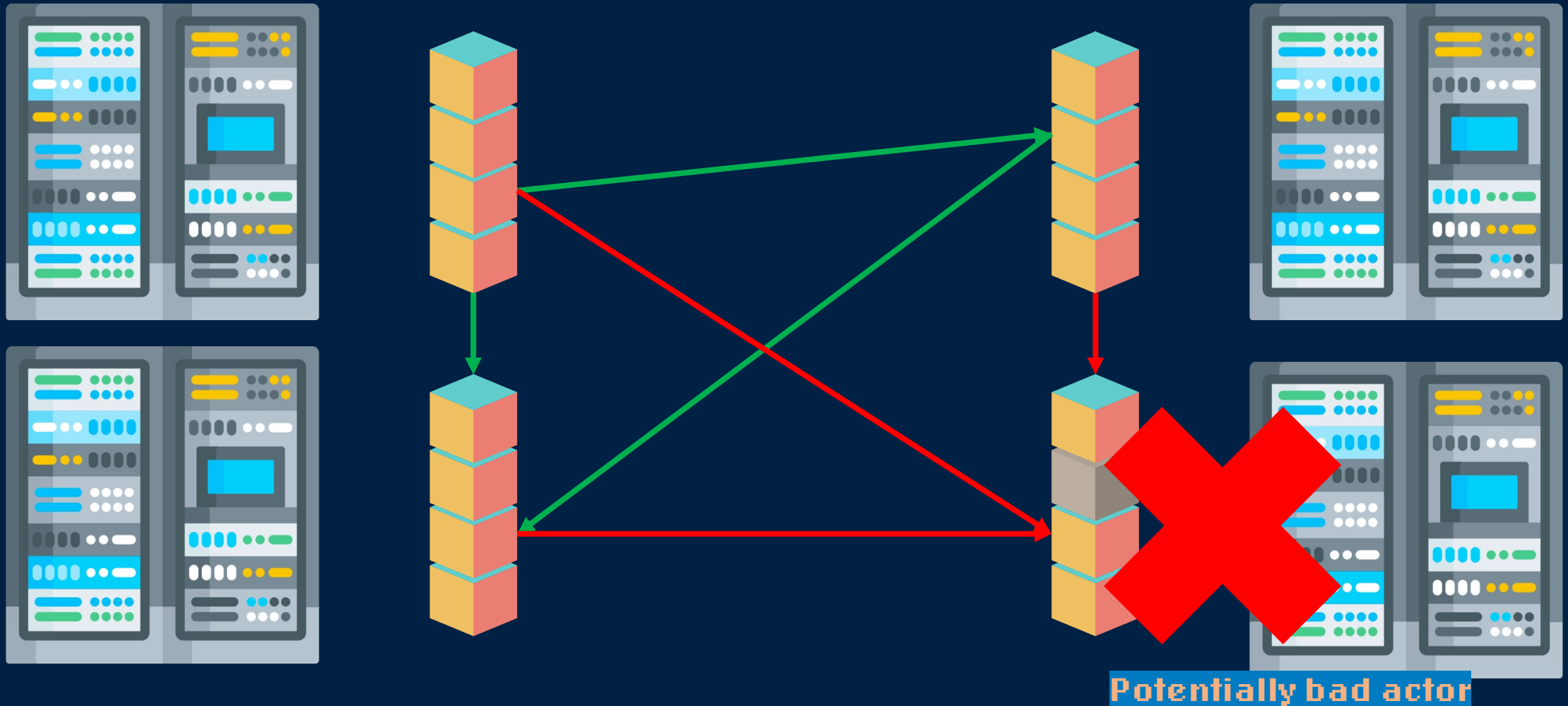
You've got your blockchain...  
I've got my hash right

- \* Hashes == mathematical summations of a block's contents
- \* V. hard to forge because they are calculated/linked to every preceding block
  - \* Are also v. long and impossible to "read"
- \* This is what differentiates a "correct" chain from an invalid one
- \* The central "truth" of a chain is referred to as a "ledger"





don't be fooled by the blocks that I got





# don't be fooled by the blocks that I got

Everyone else says



The the outlier says



Bad actors get “punished” in a chain a few ways:

- Decreased authority
- Exile from the authority pool
- Forfeit “staked” tokens
- ...



# block n' roll



- \* Blocks have incentives for authorities/processor to pay attention
- \* In the Ethereum world, this is represented by a “gas” cost attached to transactions
  - \* In contemporary versions of the platform, it’s a fee per transaction
- \* Larger transactions (i.e. more data) cost more in “gas” to power
  - \* Re: Ethereum, this is accompanied by gwei
  - \* This is the cost for paying for “gas”



# getting gassed up

<b>Estimated gas fee</b> <i>Site suggested</i> Very likely in < 15 seconds	0.00053379 <b>0.000534 ETH</b> <b>Max fee:</b> 0.00053379 ETH
<b>Total</b>  Amount + gas fee	0.00053379 <b>0.00053379 ETH</b> <b>Max amount:</b> 0.00053379 ETH

i'm in ur chainz posting  
yer dataz

\* Typically, there's also an amount you pay to a service/contract for doing something

\* For our game, you get a free ride

\* All you have to pay is gas

\* This number varies based on:

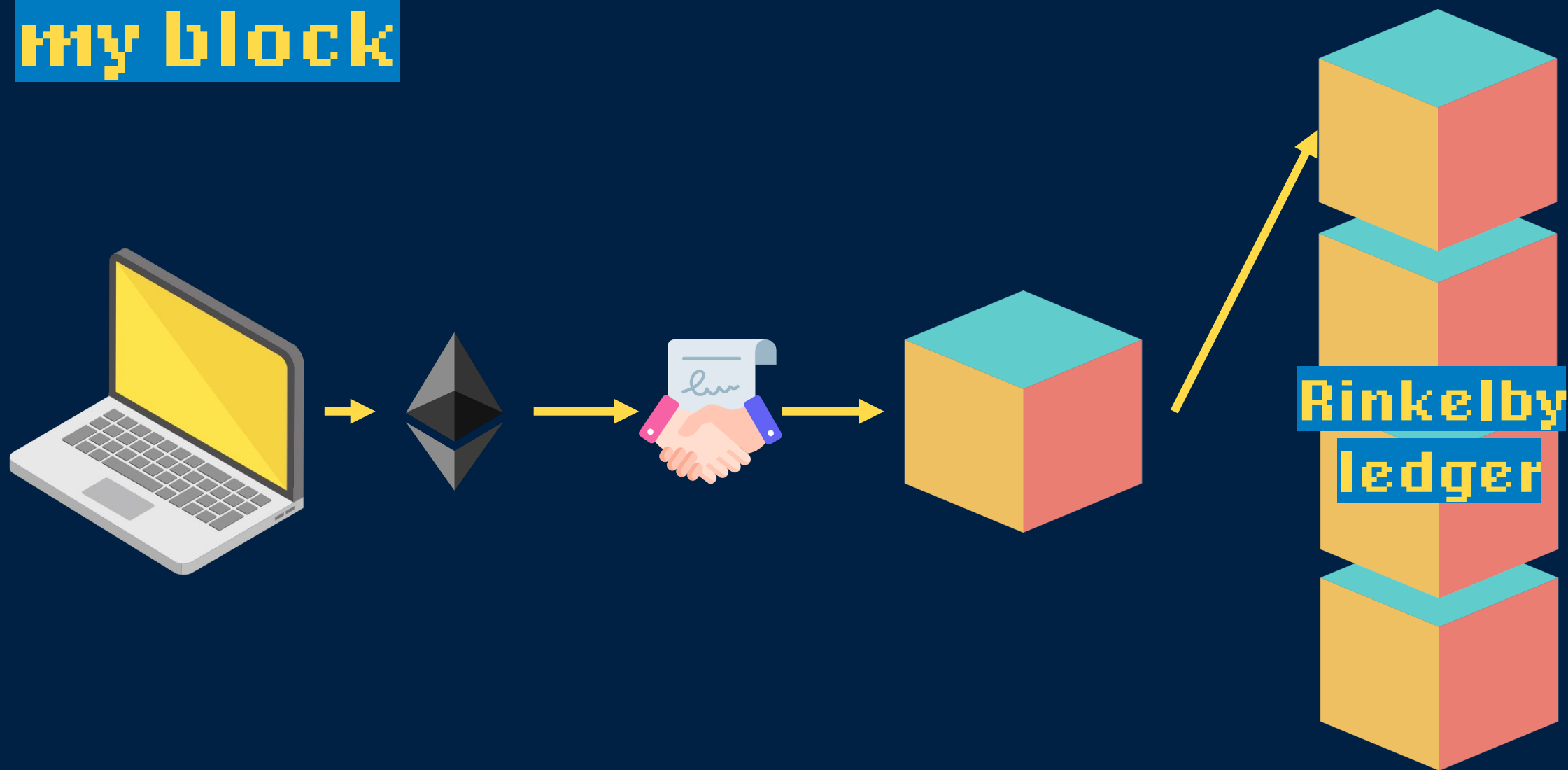
\* The amount of data transmitted

\* The cost of gas (gwei)

\* The "busy-ness" of the network



my block



Sending a transaction to the chain



my block



Rinkelby  
ledger

Reading a transaction from the chain