

# Why does bitcoin mining consume so much electricity?

**Harald Vranken**  
NDDHO, May 25, 2018



**Open Universiteit**  
[www.ou.nl](http://www.ou.nl)

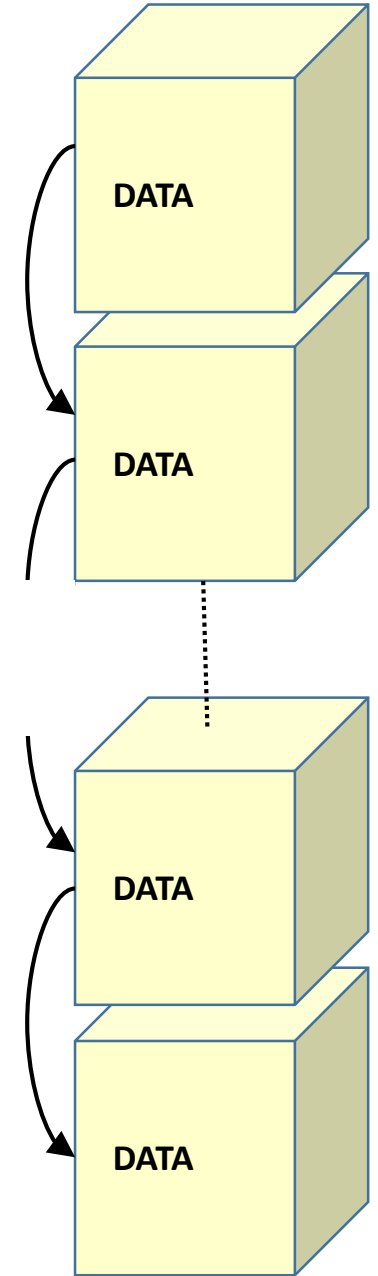


**Radboud Universiteit**



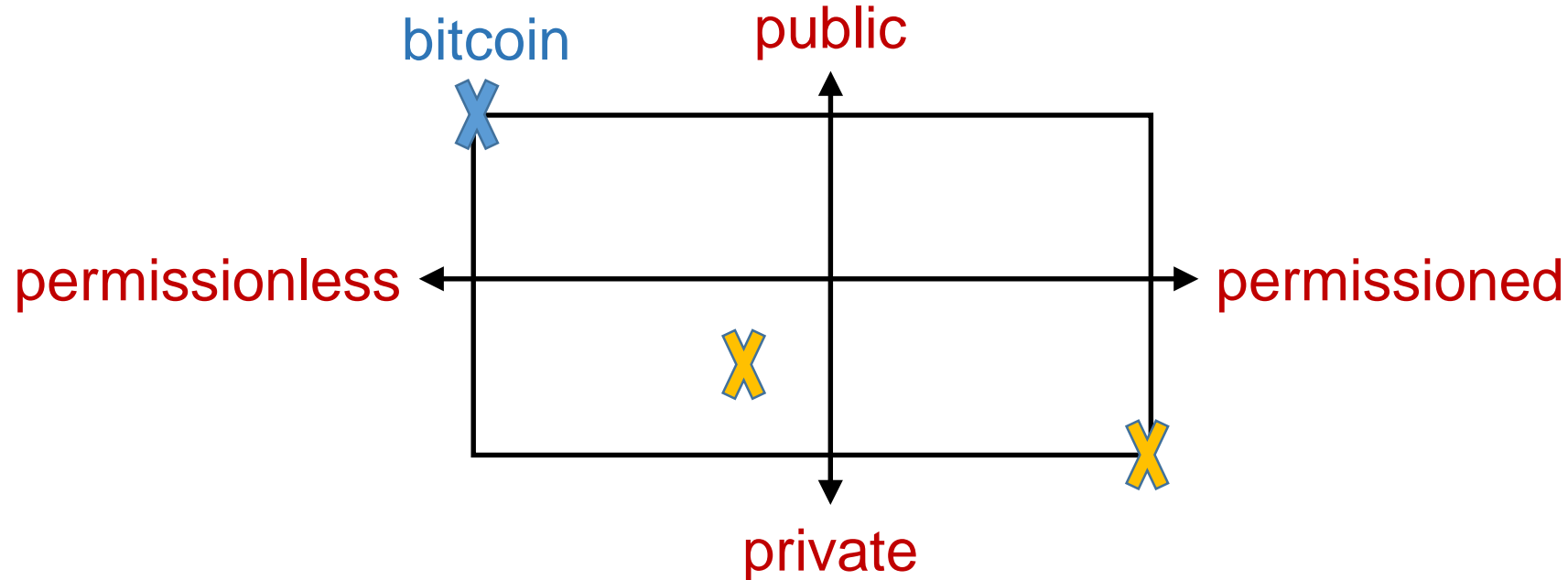
# Blockchain: definition

- Distributed, digital ledger
- Chain of data blocks
  - each block cryptographically linked to previous block



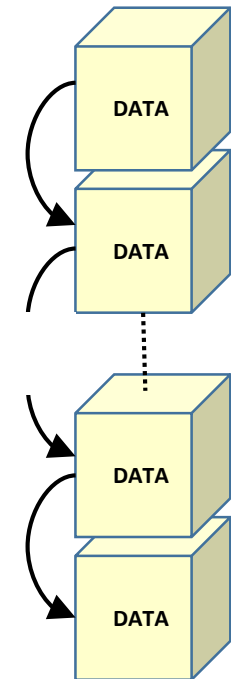
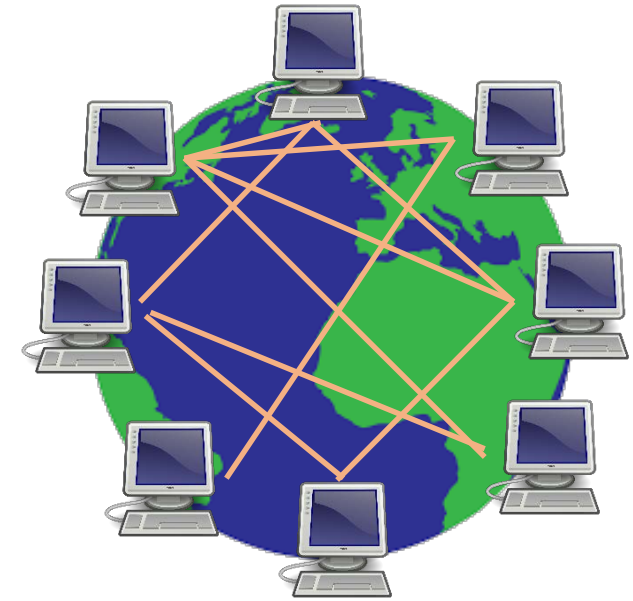
# Blockchain: types

- Public vs. private
  - restrictions on who can access (read) blockchain
- Permissionless vs. permissioned
  - restrictions on who can add/modify (write) blockchain



# Blockchain: bitcoin

- Peer-to-peer network of (untrusted) nodes
  - blockchain stores history of transactions
  - each node stores (parts of) blockchain
  - public (anyone can read)
  - permissionless (anyone can add/modify)
  - new block with transactions added every 10 minutes
- Challenges
  - How to reach consensus?  
(what transactions are stored in the blockchain)
  - How to prevent fraude?  
(unsecured transactions, double spending, tampering)

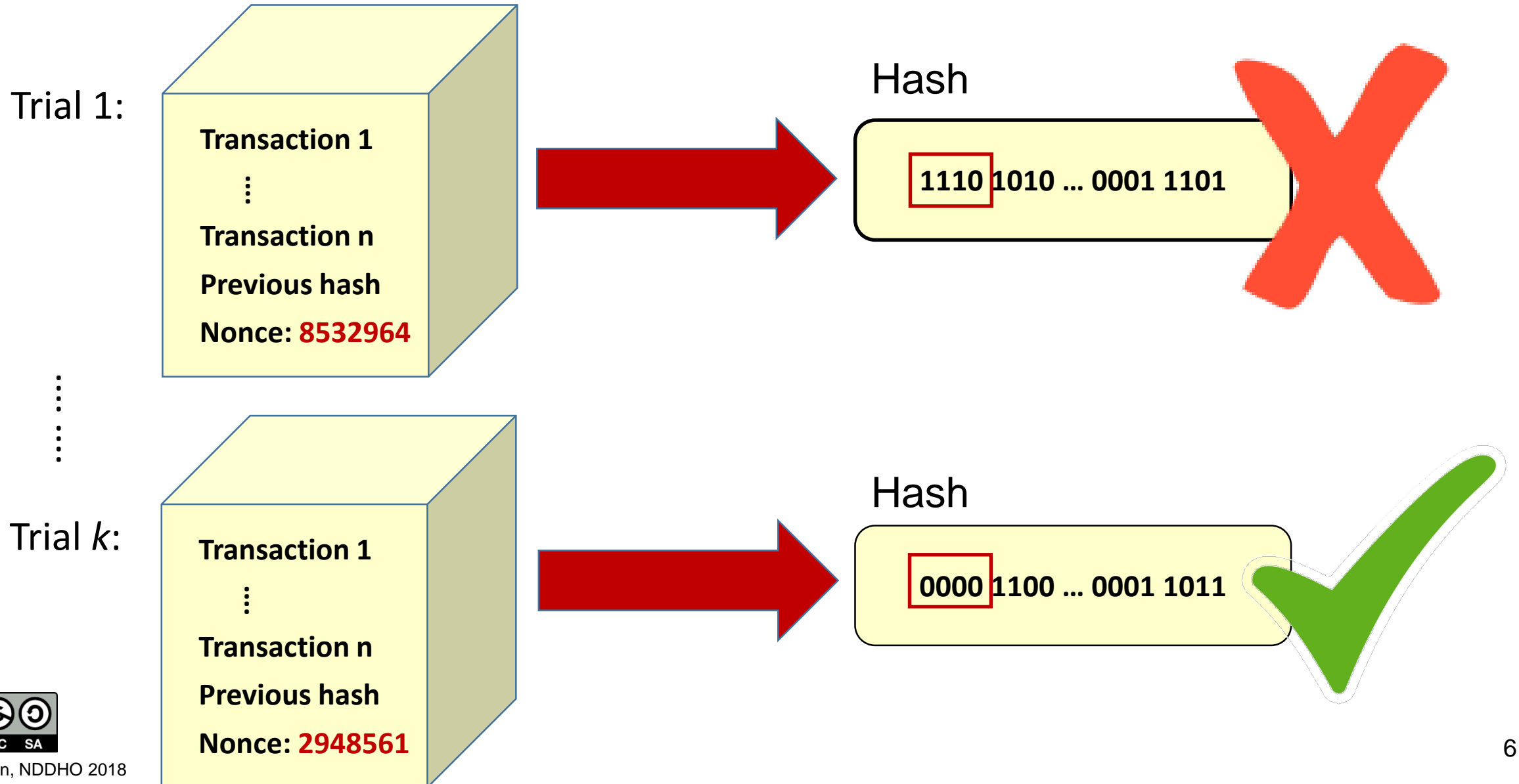


# Bitcoin: proof-of-work

- How a new transaction enters the blockchain
  1. node injects transaction into the network, received by peer nodes
  2. each node validates transaction, and propagates valid transaction further
  3. *mining nodes* collect valid transactions into block
  4. each miner tries to solve a puzzle
  5. first mining node that solves puzzle sends solution into the network
  6. each node validates solution, and adds block to the blockchain
- New block is added every 10 minutes



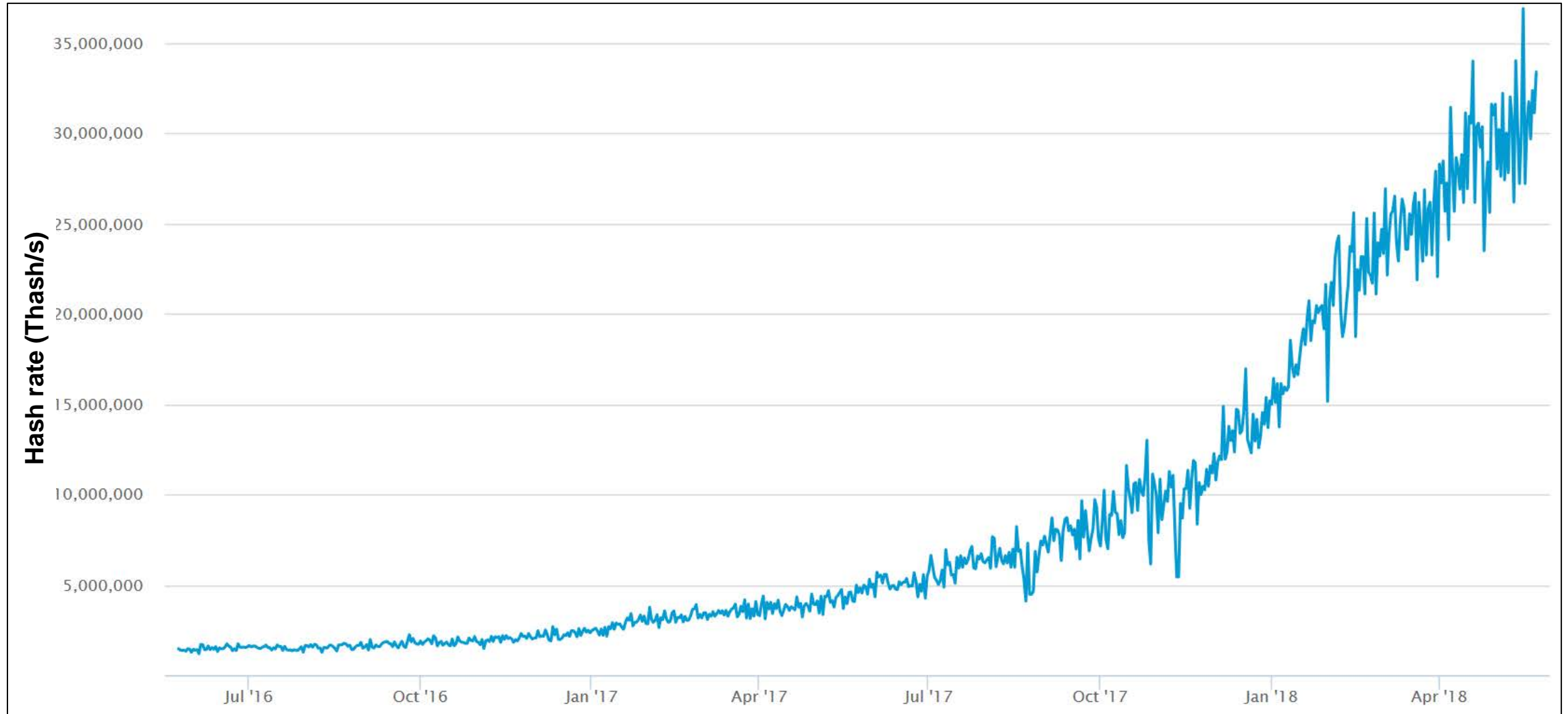
# Bitcoin: mining



# Bitcoin: mining

- How difficult is mining?
  - probability for choosing a nonce that provides valid hash  $\approx 10^{-23}$
  - finding valid hash in 10 minutes requires computing  $10^{19}$  hashes/second
- Why do miners want to put effort in computing hashes?
  - first miner who finds nonce receives block reward (newly issued bitcoins) and transaction fees for transactions included in block
- Every miner tries to be first
  - apply more, and more powerfull computers

# Bitcoin: mining



Source: [blockchain.info](https://blockchain.info)





# Bitcoin: mining

- Catch
  - miners speed up by applying more and more compute power
  - bitcoin requires pace of one new block every 10 minutes
  - throttle: difficulty of mining is adjusted every 14 days
- Hence
  - overall, no one really benefits from applying more compute power!
  - but it costs a lot of energy!!
- Large increase since end of 2017!



# Bitcoin: energy consumption

- How much electricity is spend on bitcoin mining today (May 25, 2018)?
  - at least 3.3 GW  
(considering hash rate and most energy efficient hardware)
  - potentially up to 7.8 GW (digiconomist.net)  
(considering break-even model for miners with (rough!) estimates of efficiency, bitcoin price, electricity price, hardware cost)
- Comparison

Country	Electricity consumption 2015 (GW)	Bitcoin mining (%)
Denmark	3.8	87 – 205
The Netherlands	13.0	25 – 60
World	2,553.7	0.1 – 0.3



# Bitcoin: future

- Bitcoin miners will continue consuming more and more energy as long as mining is profitable
- Can governments interference help?
  - miners quickly move to more miner-friendly places in case of interference
- Can sector take measures itself?  
(by switching from the proof-of-work to e.g. proof-of-stake)
  - miners would oppose since they heavily invested in mining equipment
  - security of blockchain and consensus mechanism with proof-of-stake are still issues



# Conclusion

- It seems bitcoin mining (and mining other cryptocurrencies) is here to stay
- We better make sure that mining is done using renewable energy
  - this is where governments can have an impact
- Public, permissionless blockchains based on proof-of-work indeed are a threat for circularity and sustainability
  - eg. bitcoin now consuming 3.3 – 7.8 GW!
  - but fortunately, not all blockchain applications are public, permissionless
  - (and also: for many applications you really don't need a blockchain...)

