Proof of Stake

Recap

- Bitcoin Incentives
- Block subsidy
- Transaction fees

Recap

- Proof of Work
  - Mining
- Transactions
  - UTXO
- Nakamoto Consensus
  - Longest chain

Recap

- Scripting
  - Bitcoin Stack Machine

Recap

- Ethereum

- Ethereum Virtual Machine

Recap

- Turing Complete
  - Solidity
- Halting Problem
  - Gas
- Smart Contract
  - DApps
  - DAO

Recap

- Proof of Work
  - Computational cost
- Attacks
  - 51% Attack
  - Longest chain
- Diminishing Block Subsidy

Proof of Work

- Central to what we saw

- What are the emergent properties?

Energy Footprint

Annualized Total Footprints

Carbon Footprint	Electrical Energy	Electronic Waste
34.73 Mt CO2	73.12 TWh	11.13 kt
		
Comparable to the carbon footprint of **Denmark**.	Comparable to the power consumption of **Austria**.	Comparable to the e-waste generation of **Luxembourg**.

digiconomist.com

Energy Footprint

Single Transaction Footprints

Carbon Footprint

292.02 kgCO2

Equivalent to the carbon footprint of **730,046** VISA transactions or **48,670** hours of watching Youtube.

Electrical Energy

614.78 kWh

Equivalent to the power consumption of an average U.S. household over **20.78** days.

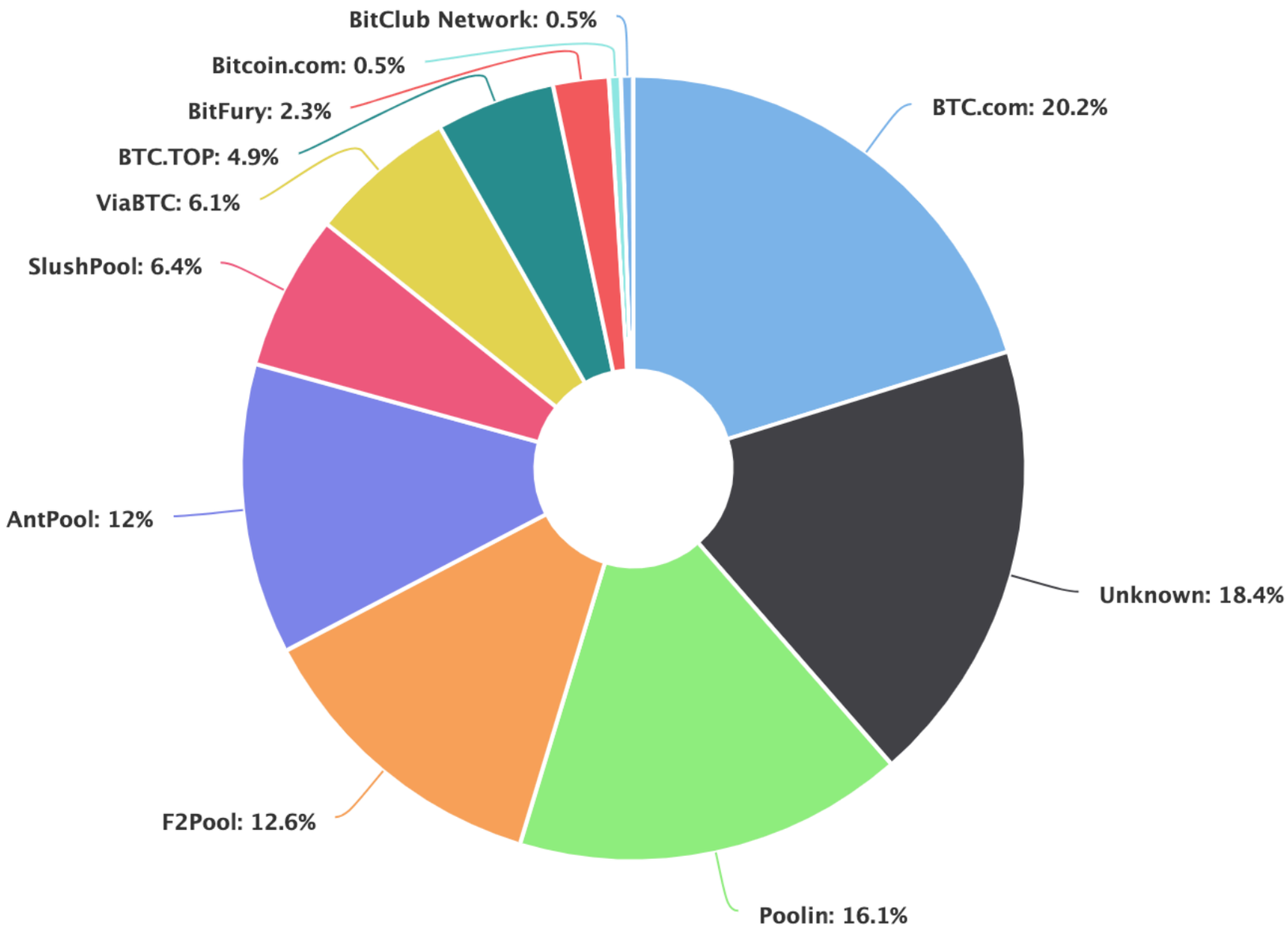
Electronic Waste

93.50 grams

Equivalent to the weight of **1.44** 'C'-size batteries or **2.04** golf balls.

digiconomist.com

Centralization



btc.com

Centralization

- ***SIGNIFICANT*** chunk of blocks mined by a few pools

- Worse as block subsidy drops

Time

- SegWit and Lightning are good steps
- Ethereum?
- ~ 15 txns per second
- (VISA: ~2k per second)
- But high activity can bring things to a crawl

Time

- Cryptokitties
- 6x increase in txn queues
- With finality?

Proof of Work

- Computational Cost
  - Arms race
- Energy consumption
- Centralization
  - Pools
- More?
  - Time

Proof of Work

- PoW uses:
- Computational Cost
- Expensive to Solve
- Easy to Verify

Proof of Work

- Avert Sybil Attack
  - Spawn a large number of fake identities
    - For influence
- PoW makes mining expensive
  - Multiple identities mean zilch w/o compute

Alternative?

- Goal:
  - Avert sybil attack
- Avoid:
  - Computation cost

$$

USE THE COIN ITSELF

How?

- Instead of proving computation power
  - Prove net worth

Proof of Stake

PoW/S

- Chance of mining
- W - Proportional to compute
- S - Proportional to net worth

The Challenge

- Easy to verify
- Hard to come up with a solution

PoW/S

- Proving:
  - W - Compute - race to discover nonce
  - S - Net Worth - just verify
    - (using your KeyPair)

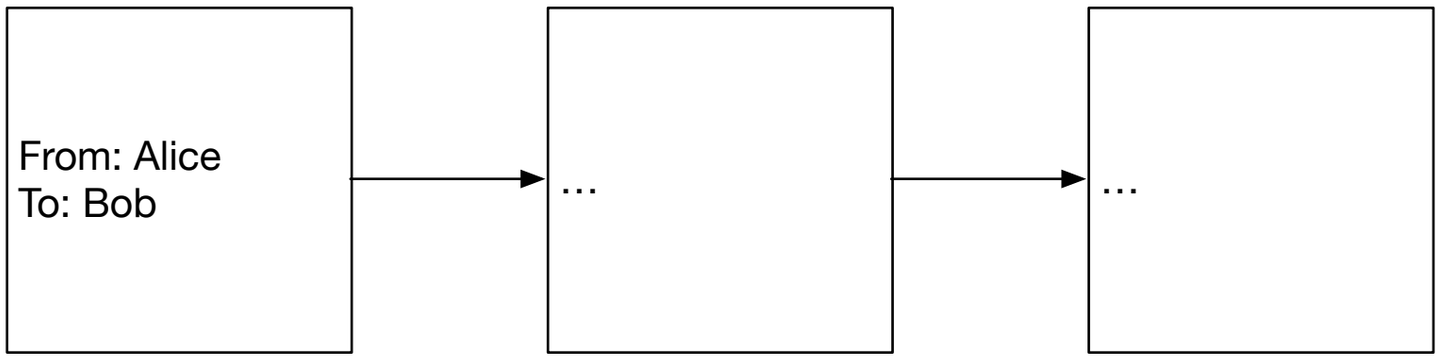
PoS

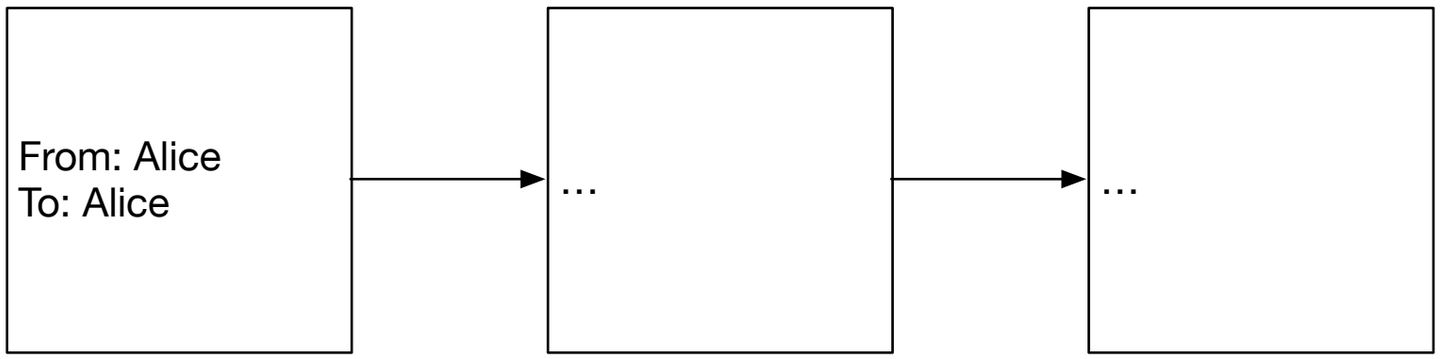
- Chance of mining
  - Proportional to your net worth (Stake)

What About Forks?

- Forks in PoW?
  - Nakamoto Consensus
- Forks Here?
  - No cost to building on both (all) forks
- Potential Double Spend
  - How?

Alice / Bob Example


From: Alice
To: Bob
…
…


From: Alice
To: Alice
…
…

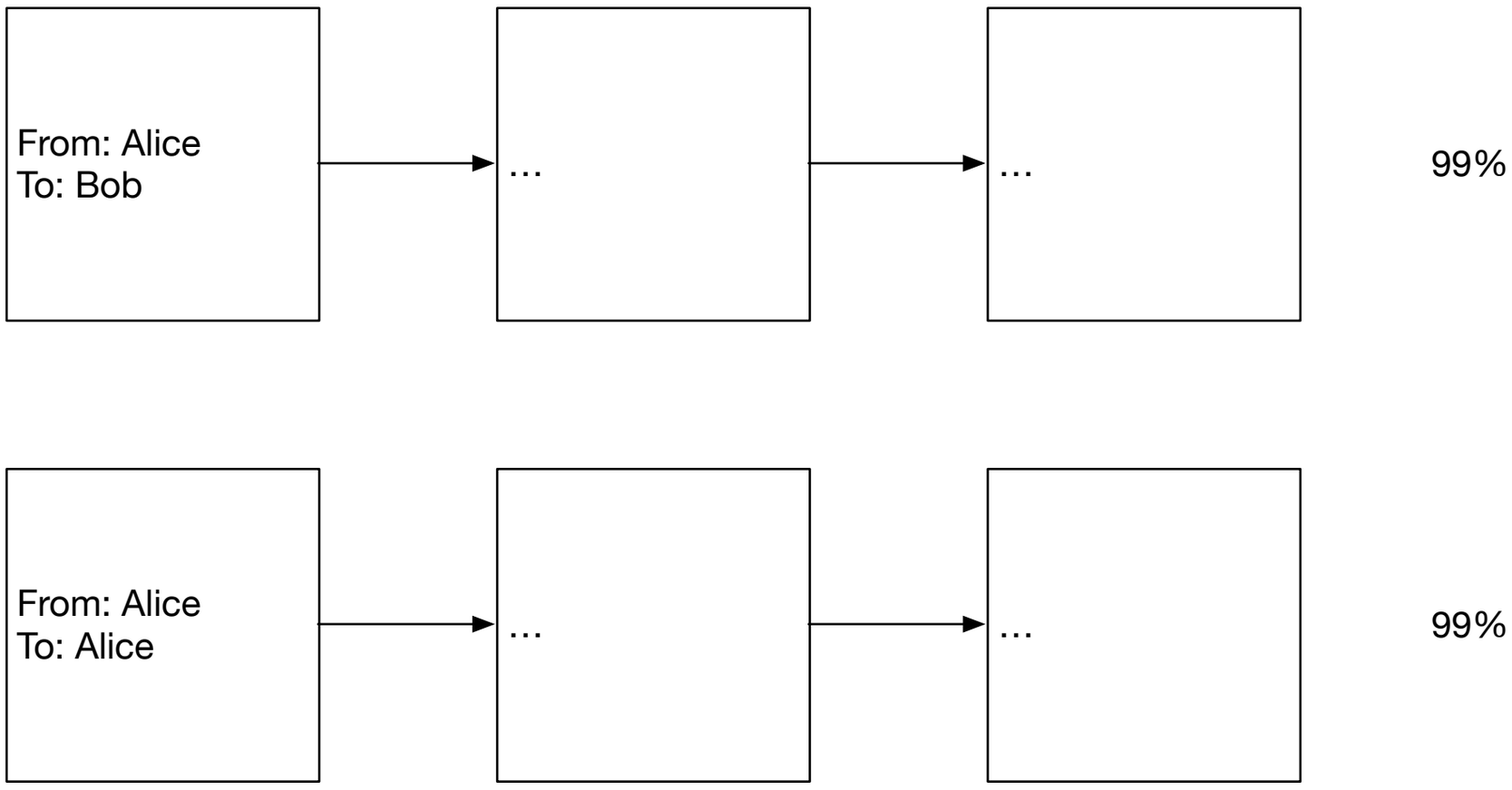
In PoW

- If Alice has >= 51%
- Alice can make the second chain longest
- And Bob is S/O/L

In PoS

- No cost to adding blocks
- Alice can just build both
- Problem
- Nothing at Stake Attack

In PoS



The 1%

- Wherever that 1% is staked wins
- Double spend

So Far

- Doesn’t seem to have happened
- Stake does count for something
  - Bad actions
  - Consequences

Finality

- Bitcoin?

Finality

- PoS?
- NXT
- Longest chain
- Bitcoin

Finality

- PoS?
- Casper
- Validators - a new type of node
- Checkpoint every 100 blocks

Finality

- PoS
  - Tendermint
    - Validators elected
    - Propose block
    - Finality every block

Tendermint Issues

- Validators known
- Can DDOS
- Chain won’t advance
  - Mitigation burden placed on validator

Proportional?

- Sample at random with probabilities proportional to stake
- Where is this randomness coming from?
  - In PoW?
  - In PoS?
- So?

RNG

- Stakes are public

- Compute power is not

Alternative

- Coin age (peercoin):
  - Only coins over 30 days old
  - Once used for proposing, age is 0
  - Reset at 90 (else you can just hold and win)

Long Range Attack

- Negligible Cost to Making Blocks
- Can just start from scratch and rewrite history
  - If you had a lot of stake in the beginning

Issues

- RNG - DDOS
- Long Range Attacks
- 1% Attack
- Stake Pool? (analogous to mining pool)

Hybrid PoW / PoS

- Peercoin
- PoW for new coin
- PoS for recording transactions

PeerCoin

- Mine using PoW
- Reward diminishes with difficulty (not height)
- PoS for new blocks
- So it transitions to PoS

Casper

- Validators
  - Stake some ether
  - Validate blocks by placing a bet on it
  - If block is appended, reward proportional to bet
  - Malicious activity punished (all staked ether burned) - Slasher

Questions?