# Ethereum-IPFS Hackathon

Seattle, 2017

# Blockchains?
# Ethereum? Whaaaa?

An Intro to Ethereum
by Dan Finlay


flyswatter


@danfinlay

# Hashes

- Arbitrary input
- Same-length output
- Should be unlikely that two inputs share an output.

input: hash:

“Hello, Seattle!” → 
89053f58ec93cd74
0e44e1a79999663d

“Hello, Seattle” → 
78c822c6b2f9cb44
62fa80e408496233

- Lets you quickly prove you have a file, given its checksum!

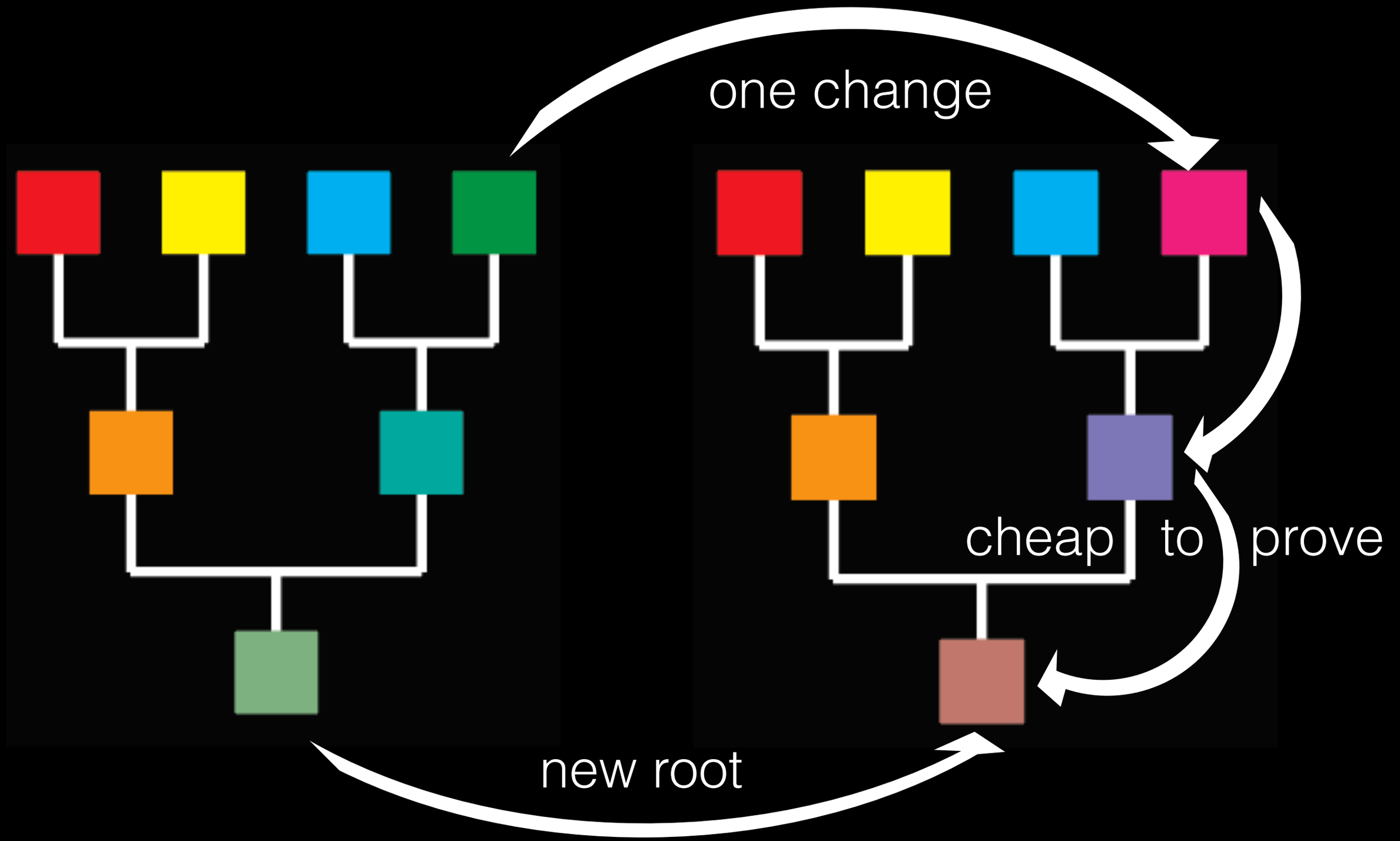
space_oddity.mp3 → 
9955f0021f91b98cb
d3f08dd49827b67

→ 
6fdf28c41257de9fc
74c33eaaae226ef

this_slideshow.ppt → 
??????????????

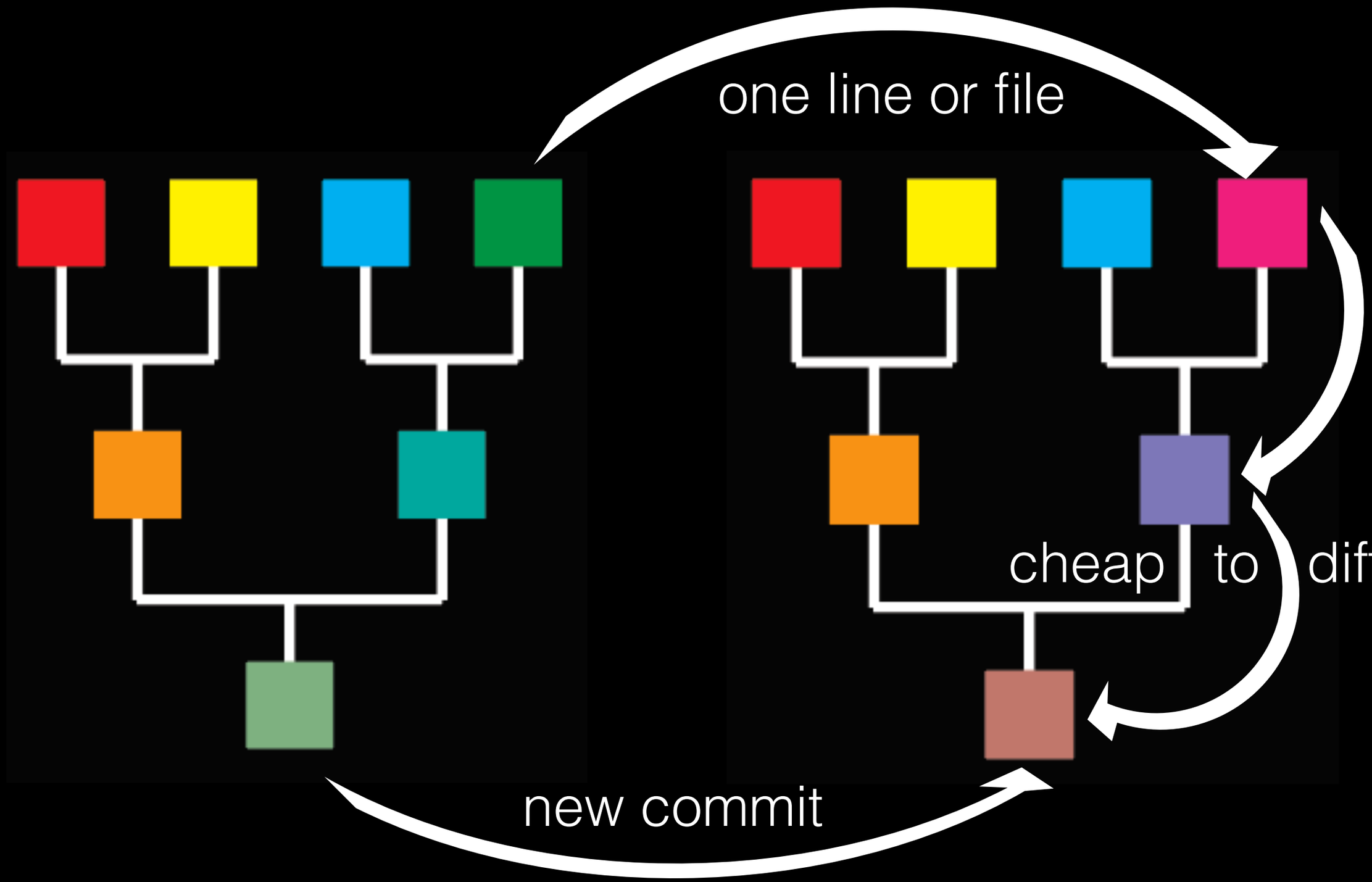
# Merkle Trees

Hashes of hashes!



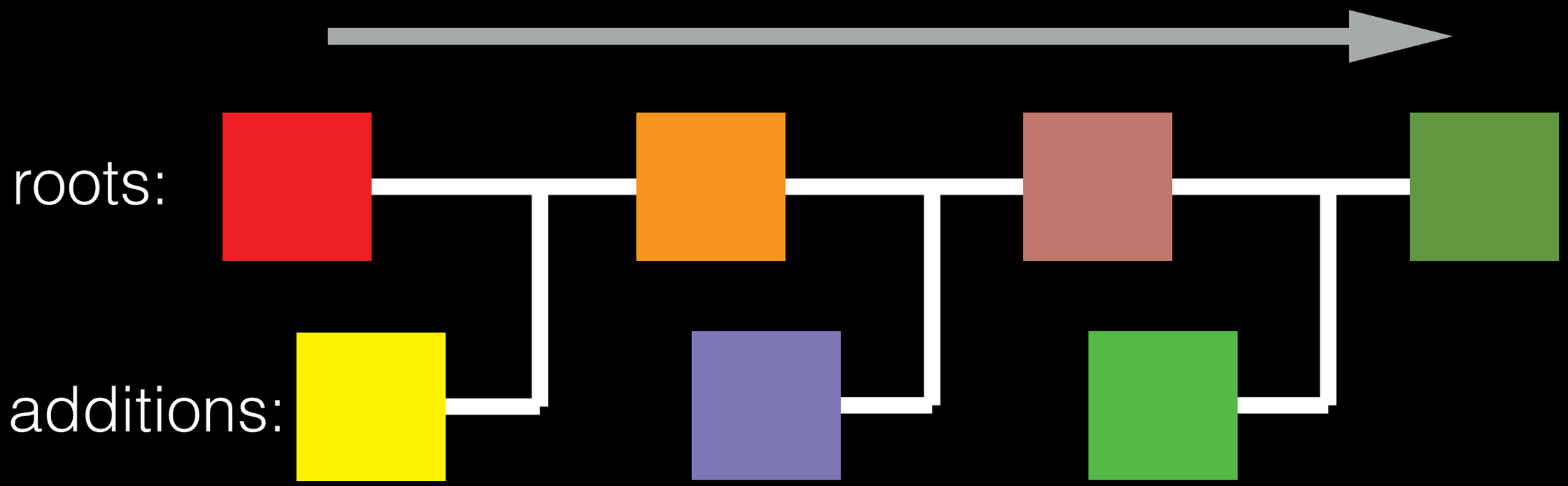
# Git

## Merklized Version Control



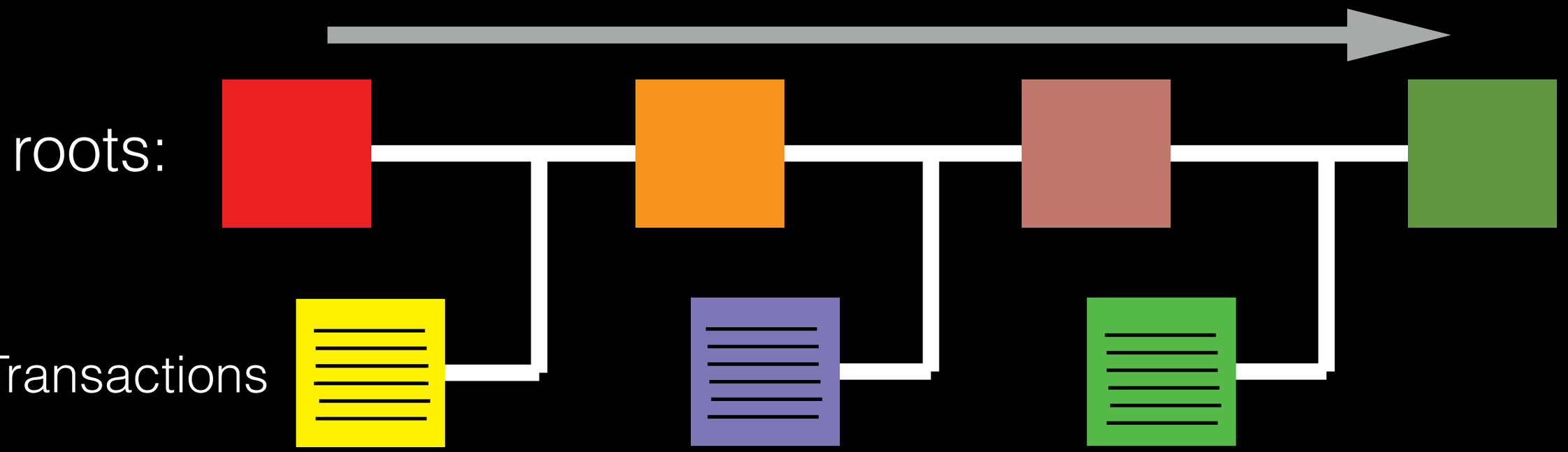
# Blockchains

## An Ever-Growing Merkle Tree



# Bitcoin

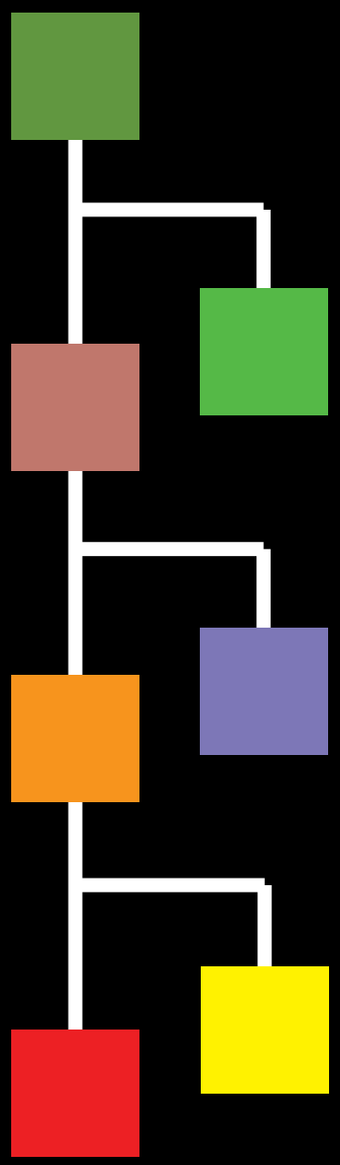
A Blockchain Ledger




Avoids double-spending
by ensuring transaction ordering.

# Reaching Consensus

How to add to a shared blockchain

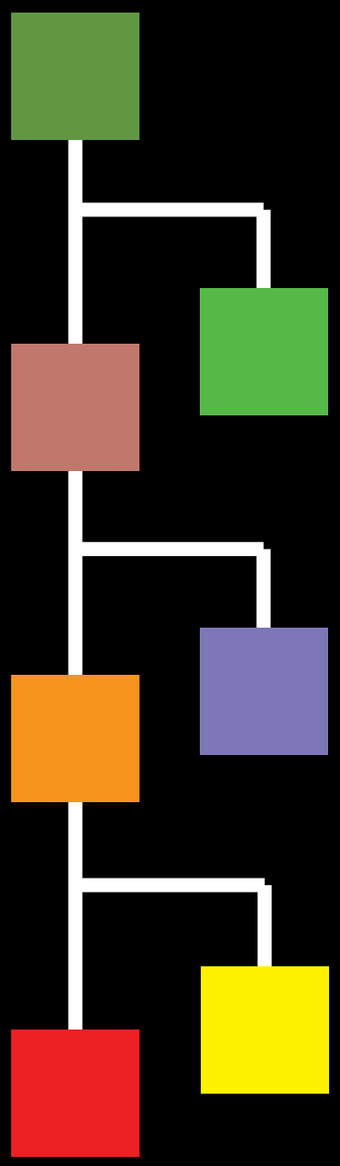


## Proof of Work

- Blocks are added gradually.
- People take turns adding blocks. (“One CPU One Vote”)
- Bitcoin style: The root checksum must start with a number of zeroes! (Difficulty)
- The block includes a nonsense “nonce” that can be changed to create new checksums.
- The difficulty is adjusted to target a desired time between blocks.

# Reaching Consensus

How to add to a shared blockchain

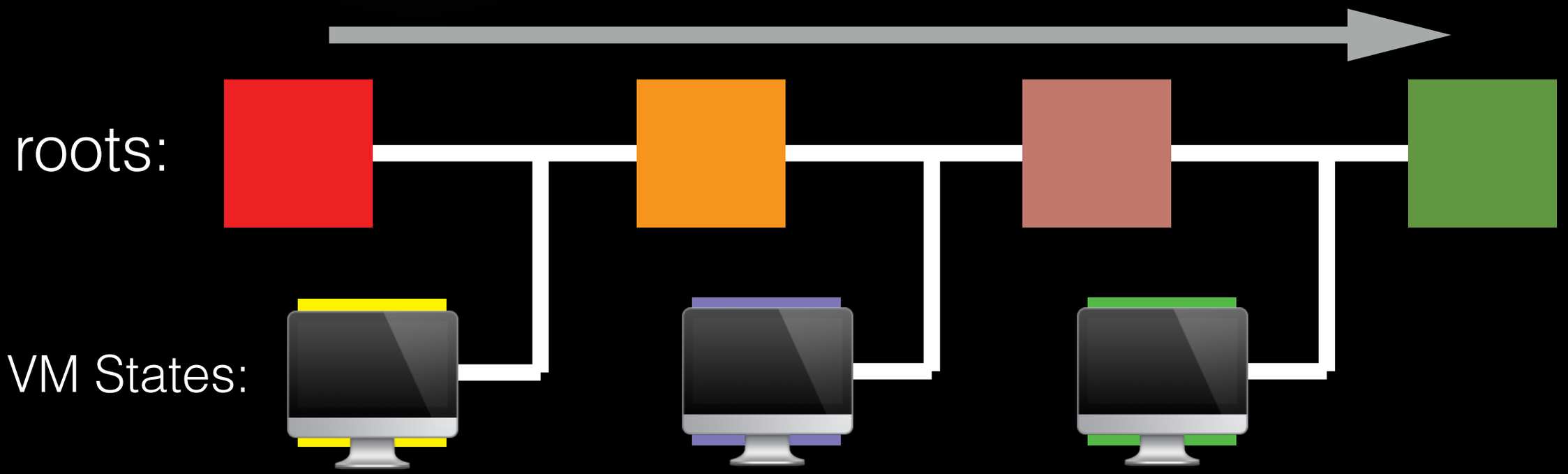


## Incentives

- The miner who finds a new block, gets a reward.
- This reward is used as currency, and to pay transaction fees.
- In addition to the block reward, the miner gets transaction fees.
- This encourages miners to process blocks with transactions.
- This encourages users to pay fees depending on urgency.

# Ethereum

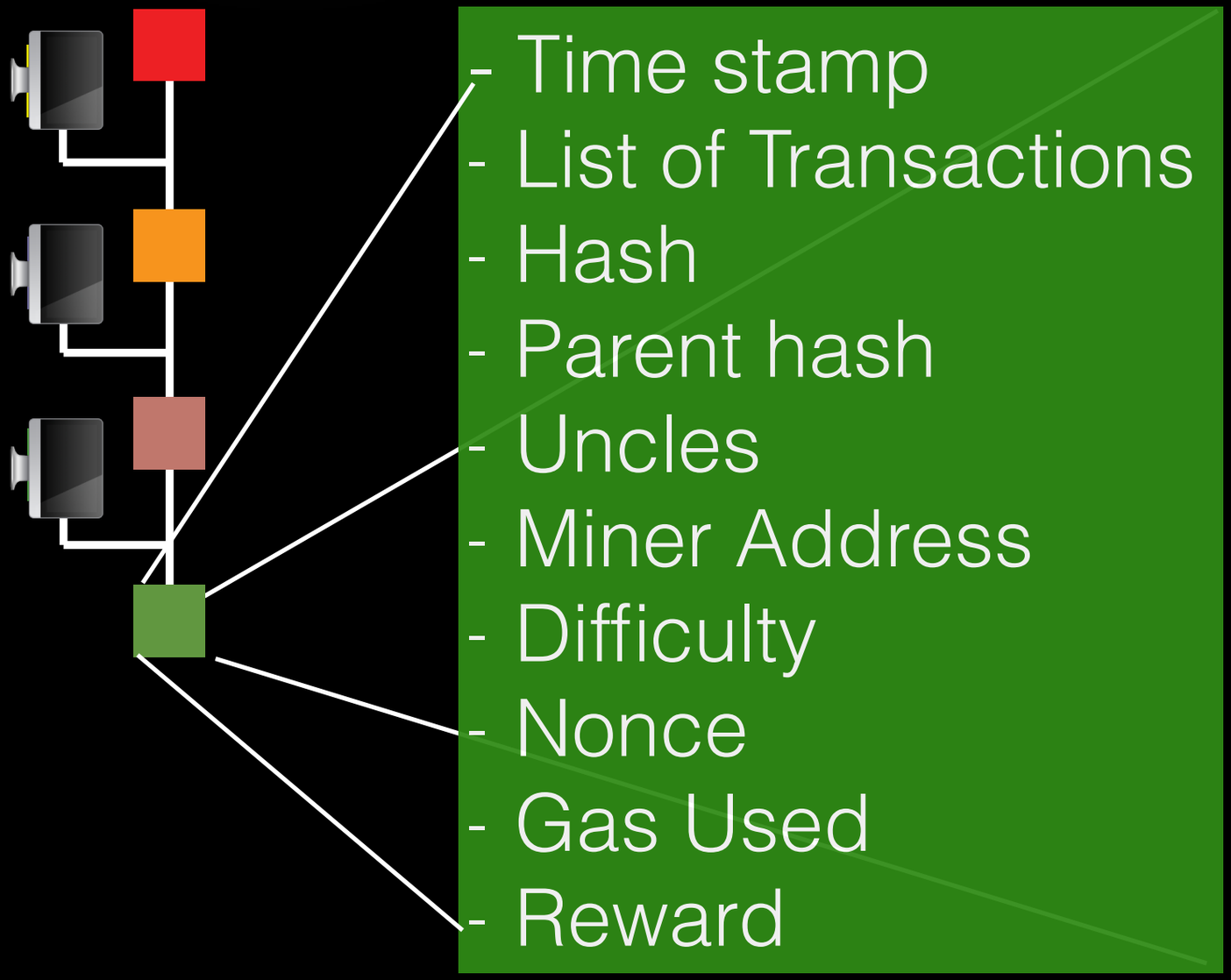
Put a computer on the blockchain

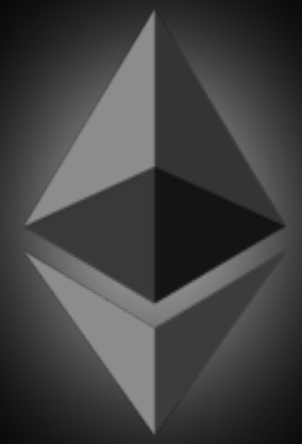



Defines a Virtual Machine
whose usage is metered
with transaction fees.

# Ethereum

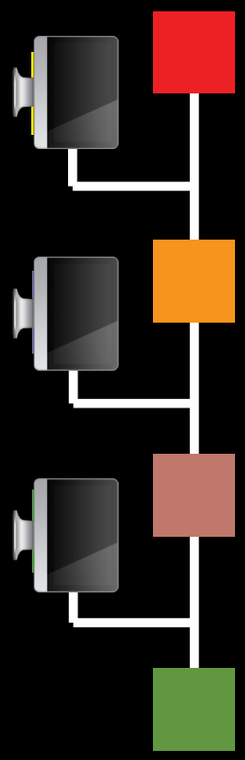
## Block Structure (partial)





# Ethereum

## Transaction Structure

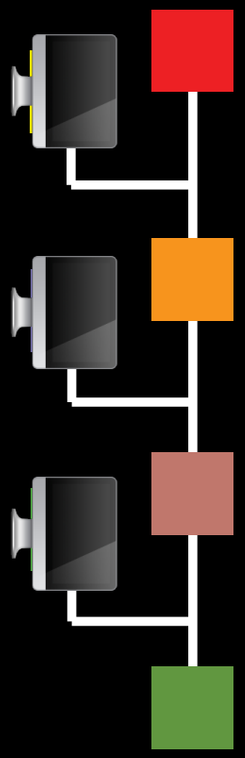


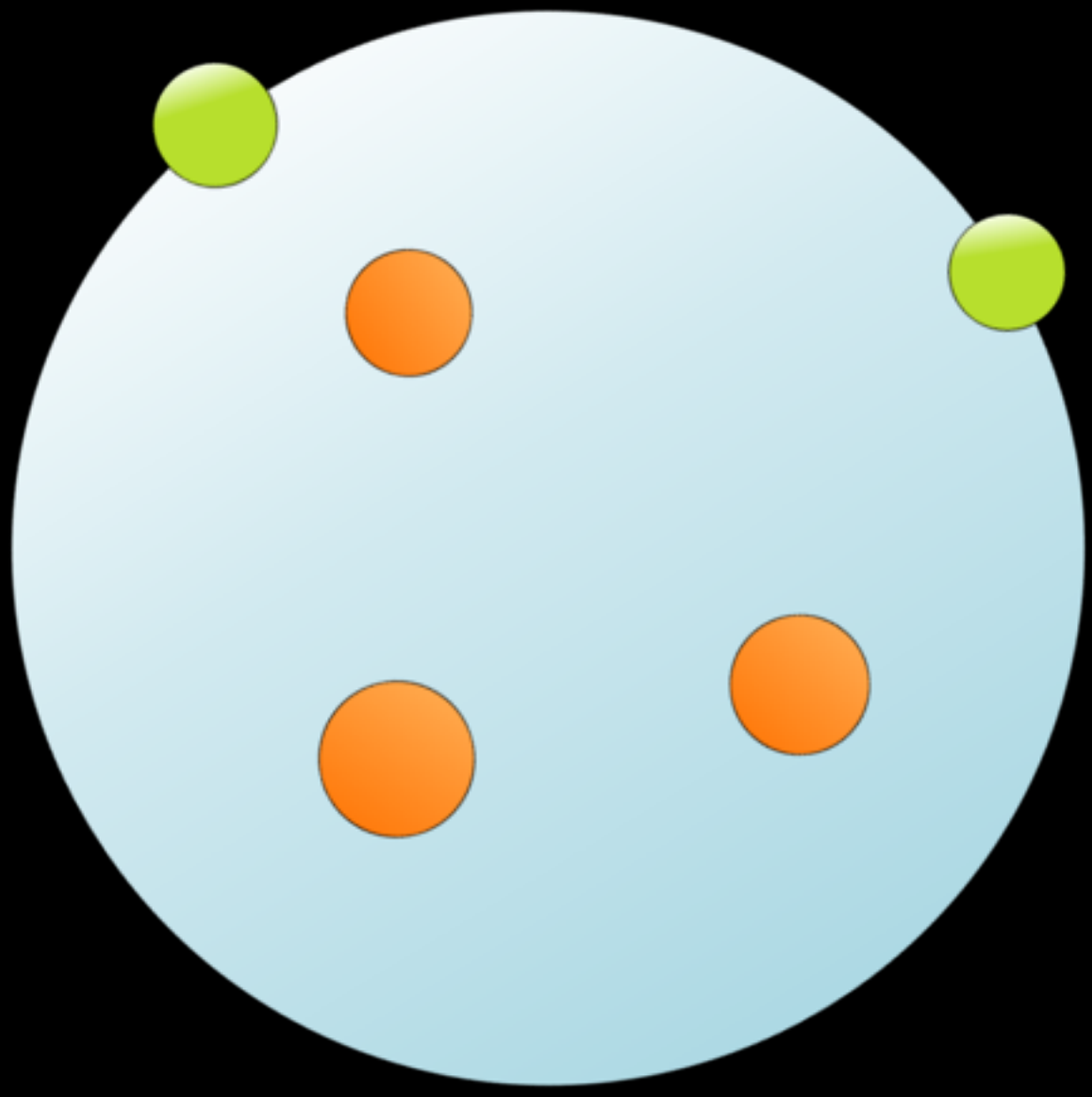
transactions

- from (address)
- to (address)
- gas price (per op)
- gas limit (for tx)
- value (sent ether)
- data (anything)
- signature

# Ethereum

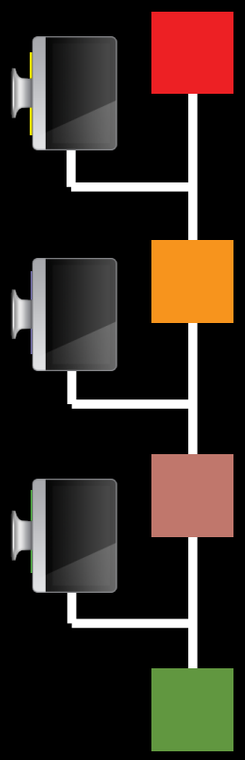
## VM State: user accounts & contracts

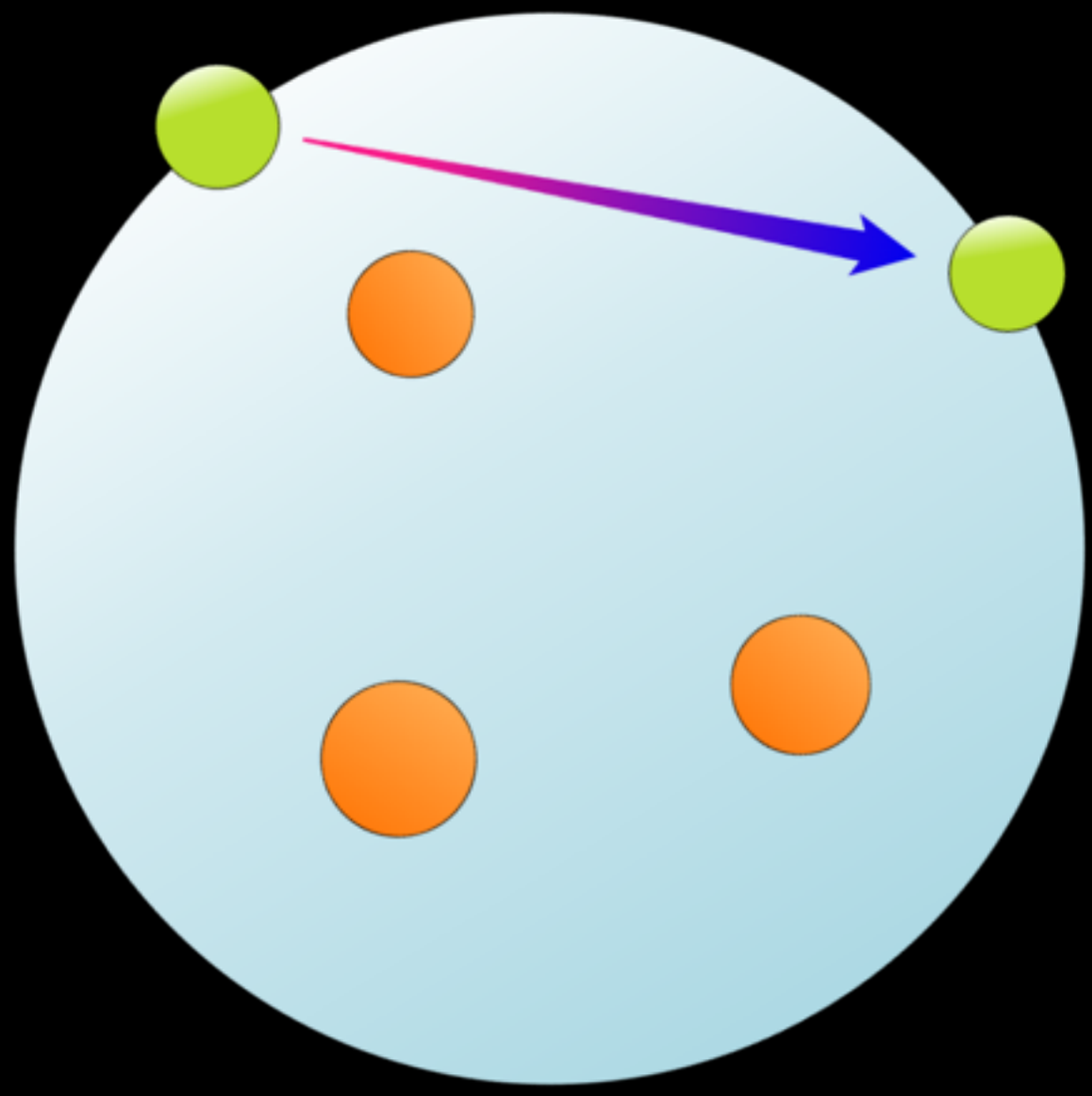




# Ethereum

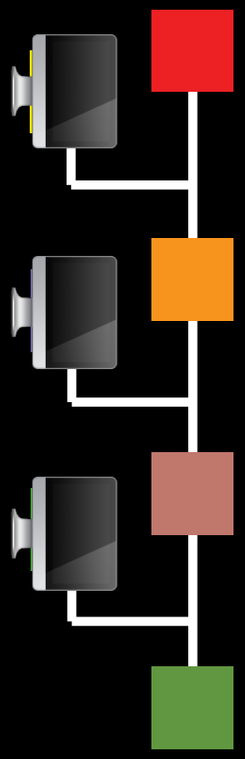
send ether between two accounts

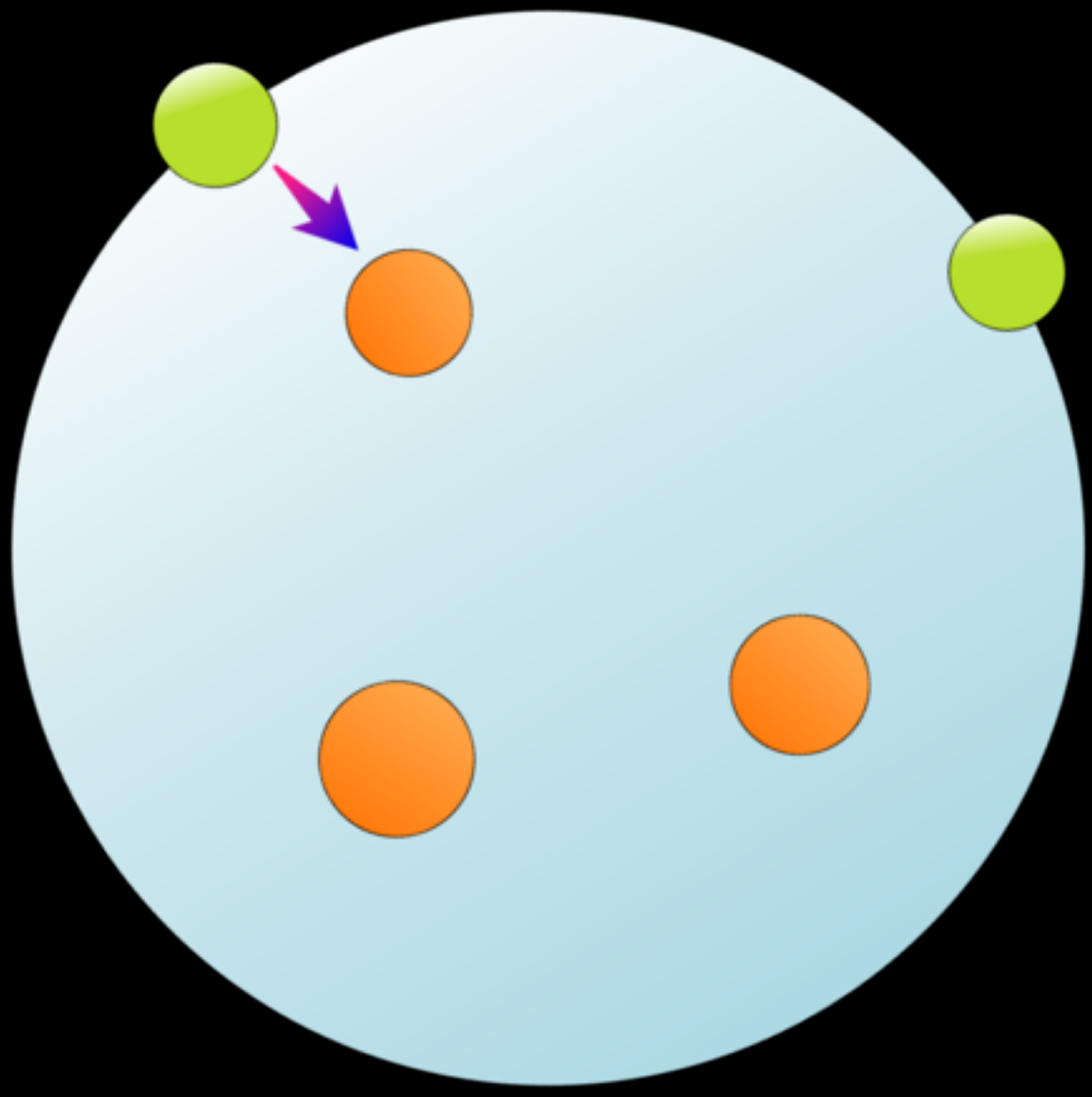




# Ethereum

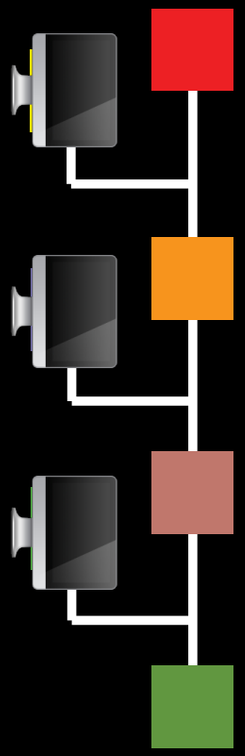
call method on a contract

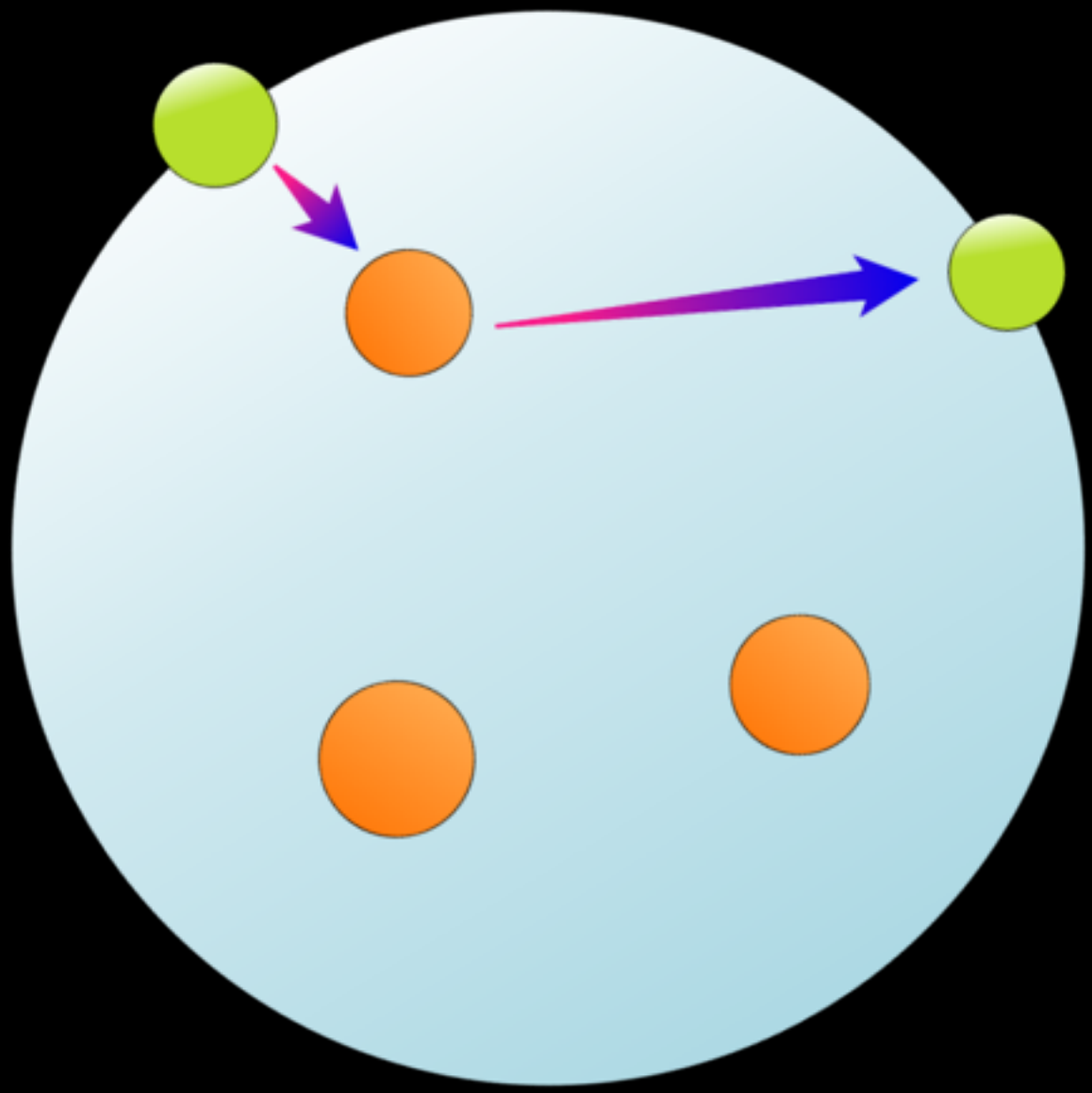


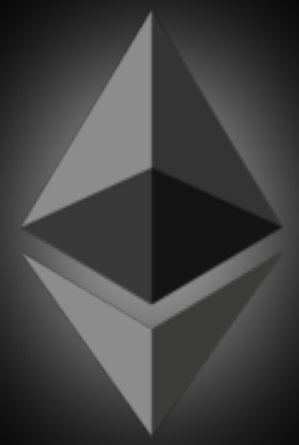


# Ethereum

contract reacts to being called

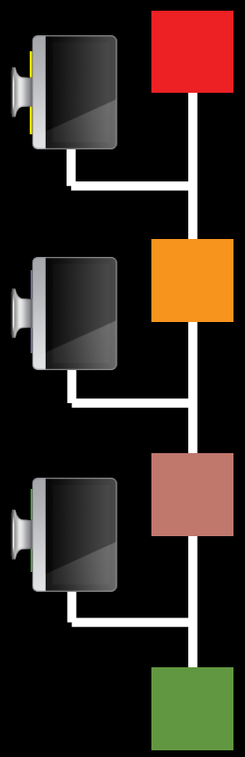


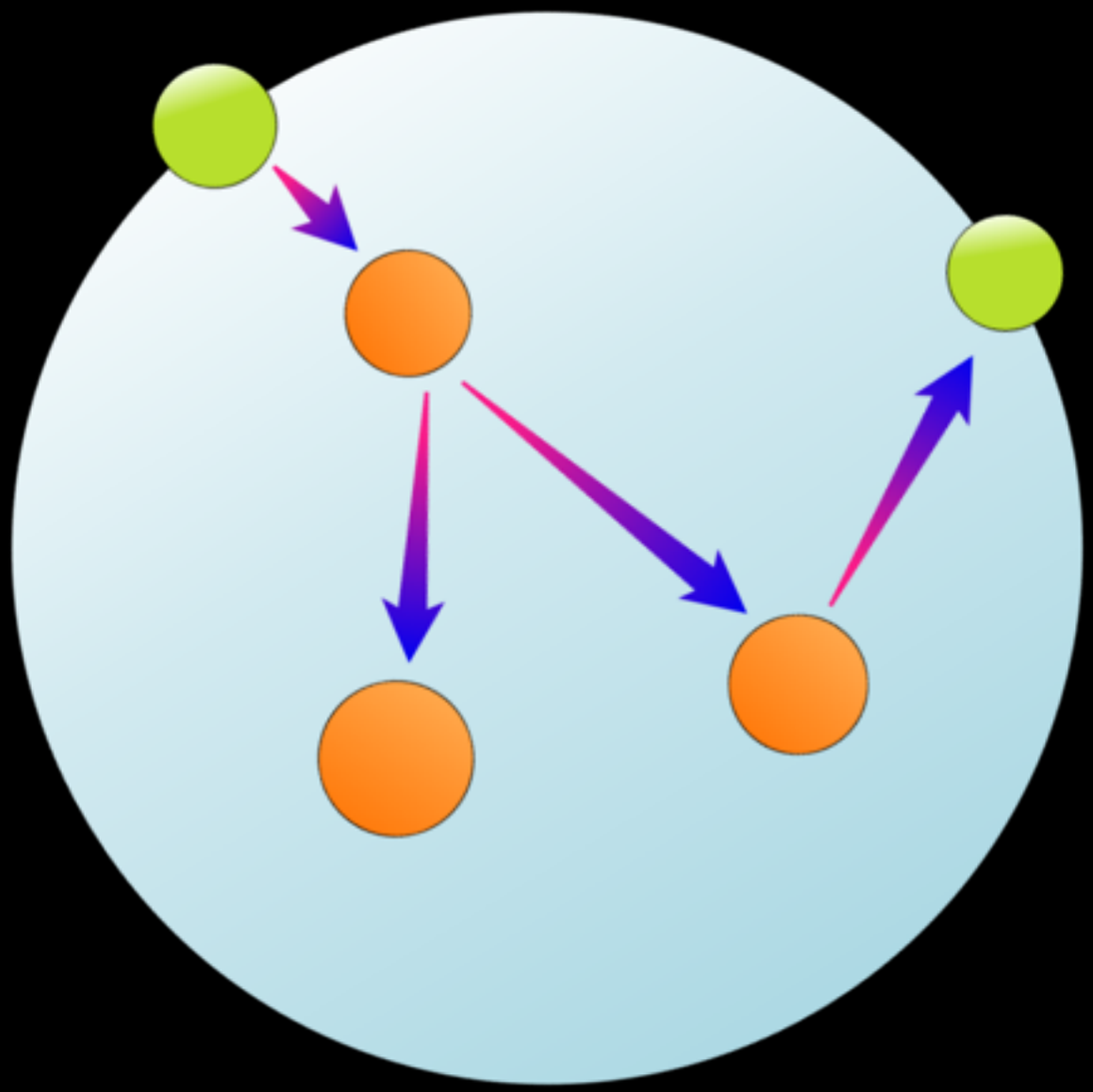




# Ethereum

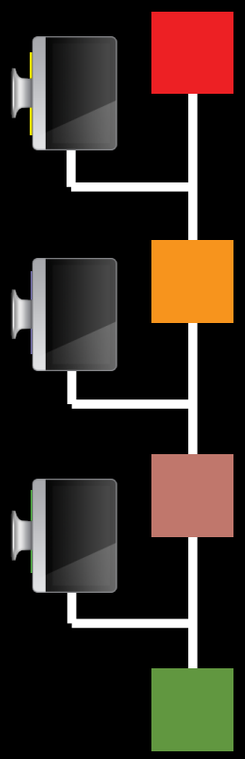
## chain reactions

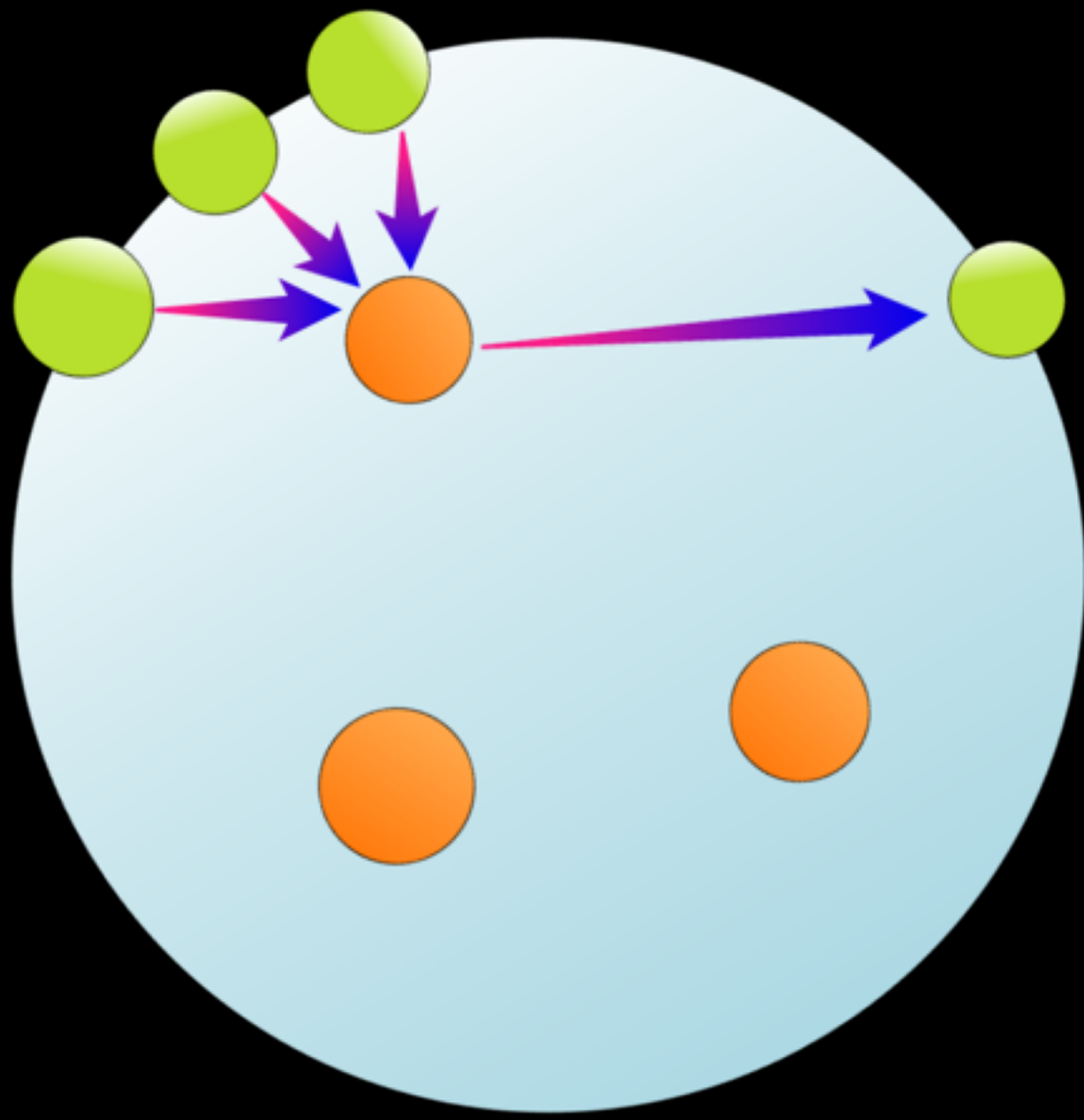


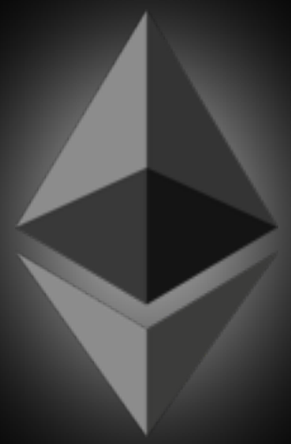


# Ethereum

## multi-sig via proxy contracts

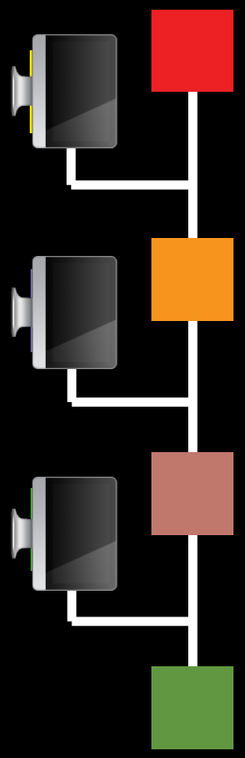


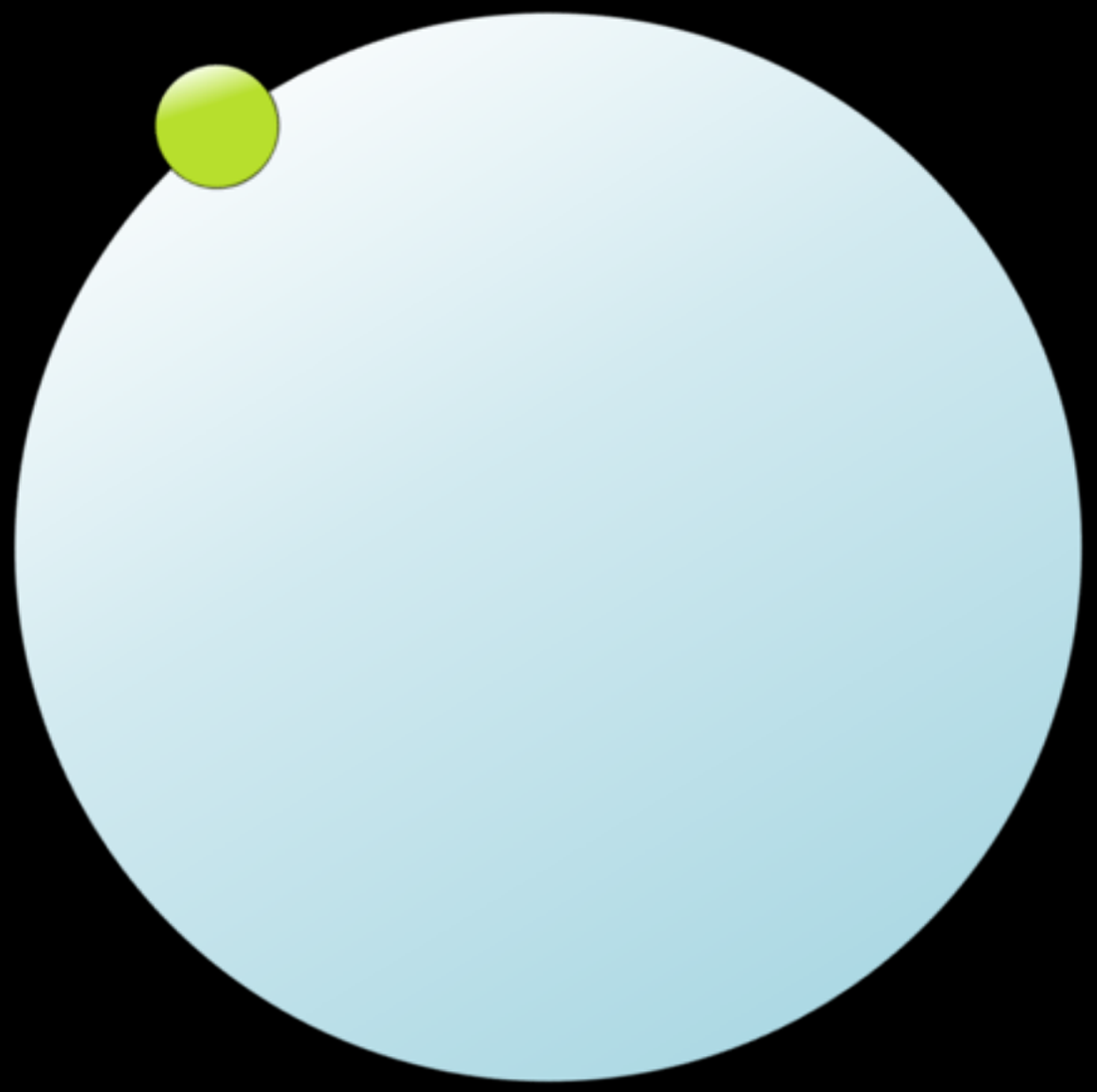


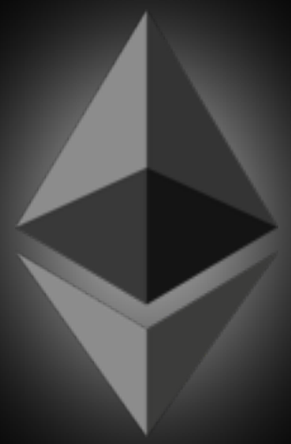


# Ethereum

## where do contracts come from?

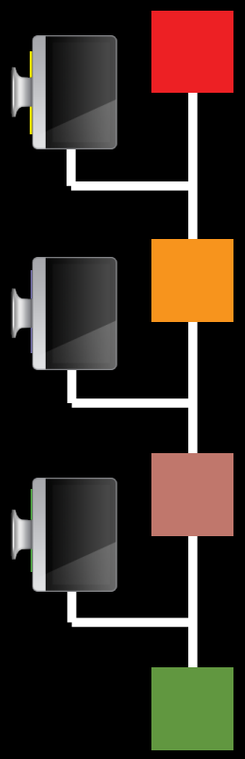


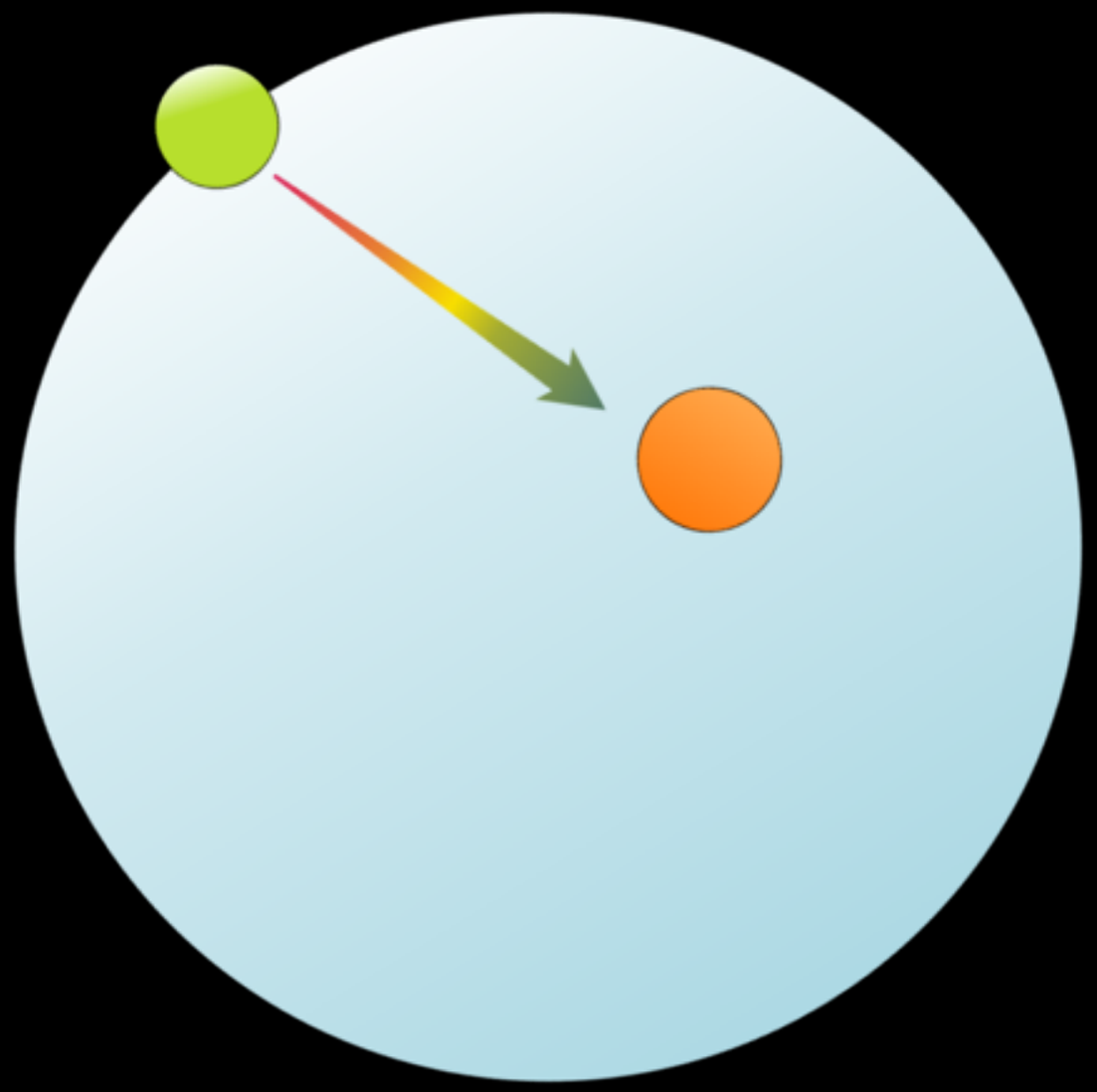




# Ethereum

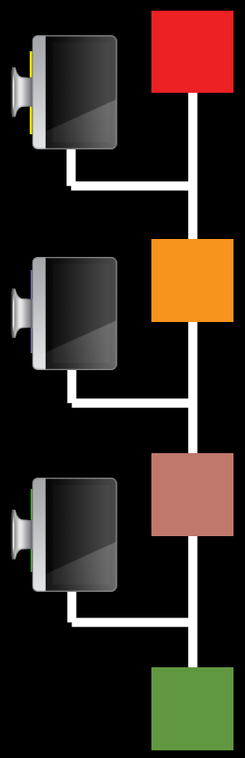
special tx (with empty ‘to’ field)
publishes data as executable





# Ethereum

## What is it good for?



WeiFund
Crowdfunding

BoardRoom
Transparent Governance

GNOSIS
Prediction Markets

BALANCE
Accounting

VIRTUE POKER
Provably Fair Gambling

Ethlance
Job Markets

MAKER
stable currencies

p2p Exchanges

ujo MUSIC
p2p art ownership

ETHERLOAN
p2p lending