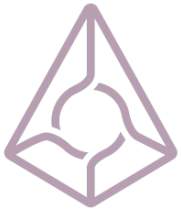
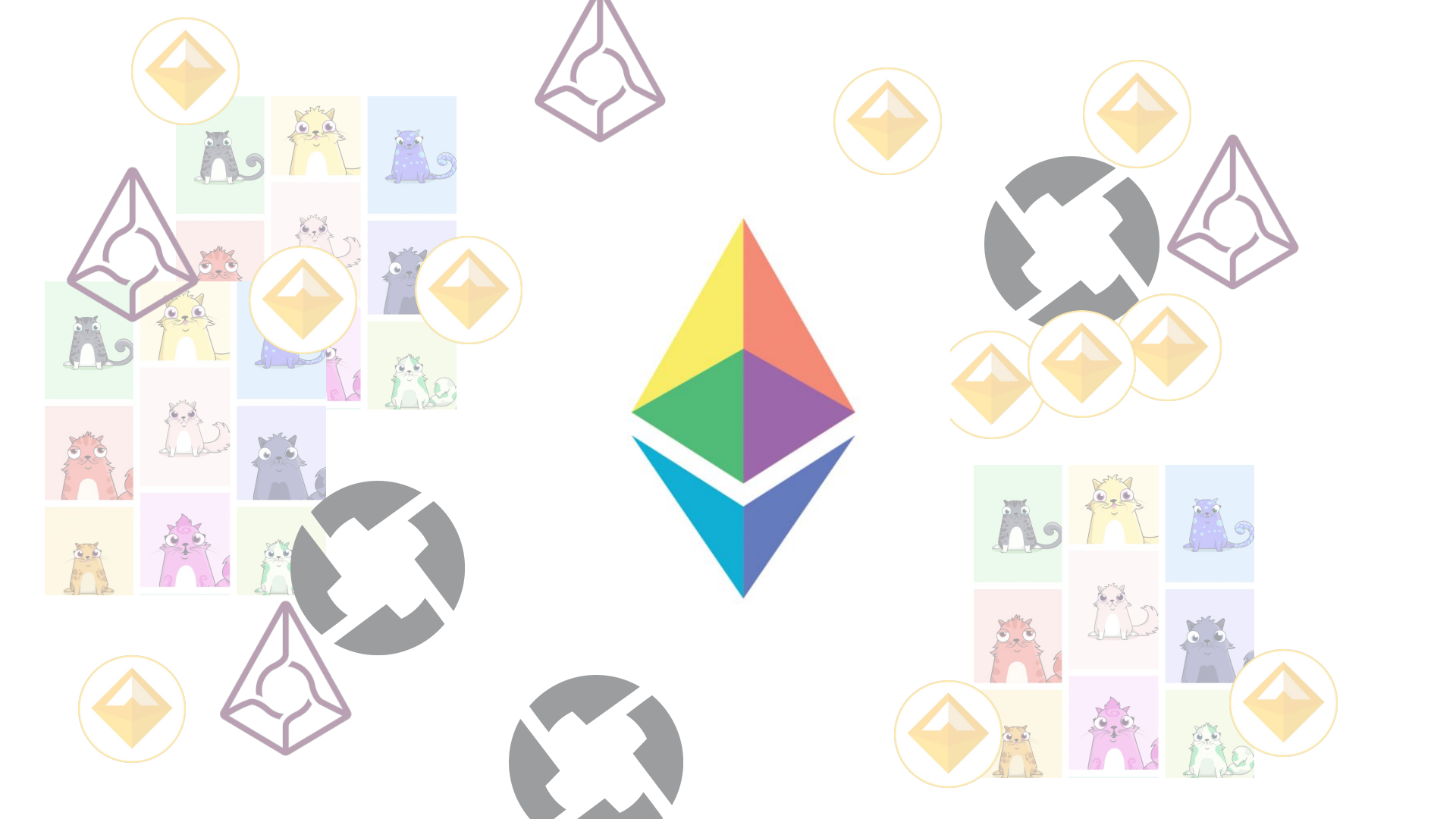
The finality gadget

Putting eth2.0 to work…

Alex Stokes
(@ralexstokes)

ethereum





Ethereum 2.0

- Building on several years of research to scale Ethereum

- Constellation of updates
  - Proof-of-stake consensus
  - Scalability with sharding
  - More flexible, safer smart contracts

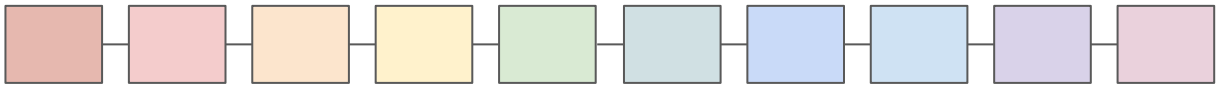
Ethereum 2.0

- Phased deployment
  - Easier to manage complexity

- Phase 0
  - Beacon chain
- Phase 1
  - Shard data chains
- Phase 2
  - Shard application chains

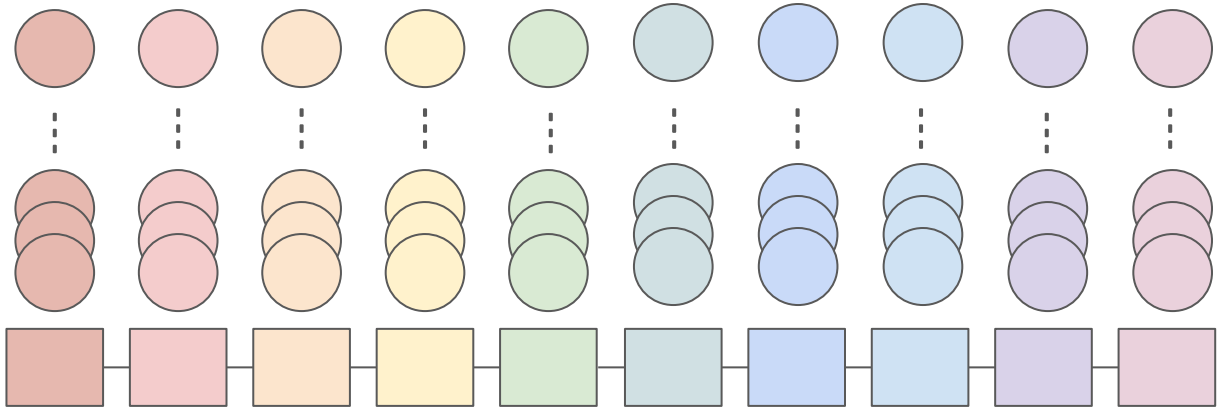
Eth2.0: phase 0

- Beacon chain
  - System-level blockchain
  - Casper proof-of-stake consensus
  - Empty references to shards



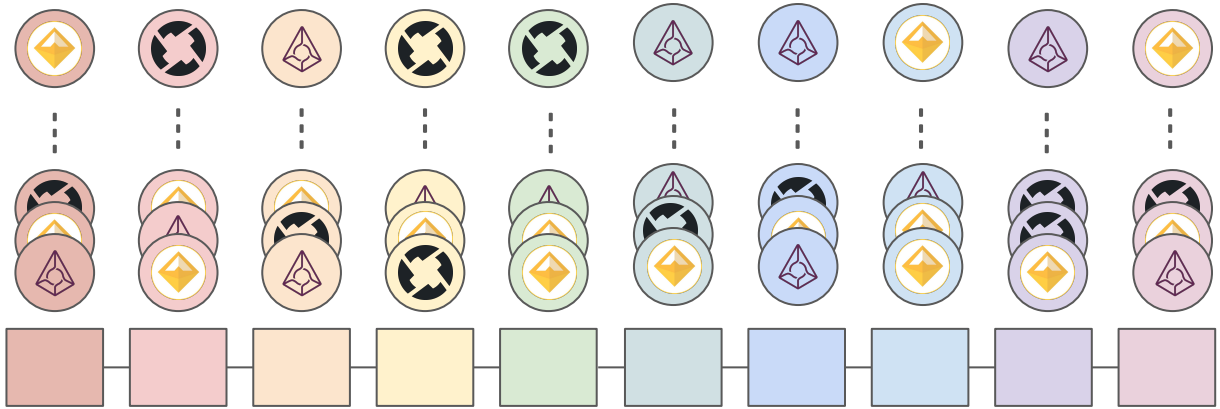
Eth2.0: phase 1

- Shard data chains
  - Add 1024 shards
  - Blocks just have 16kB of random data
  - Canonical shards are “crosslinked” into the beacon chain



Eth2.0: phase 2

- Shard application chains
  - eWASM VM
  - Flexible ‘execution environments’



when?

- When it is ready 😉

Ethereum 1.x

- Eth2.0 will take some time to safely deploy

- Bundle of improvements to Ethereum today to keep the network running
  - State management
  - Updates to the EVM
  - **Finality gadget**

- Other ways eth2.0 can help eth1.x (, but that’s a different talk)

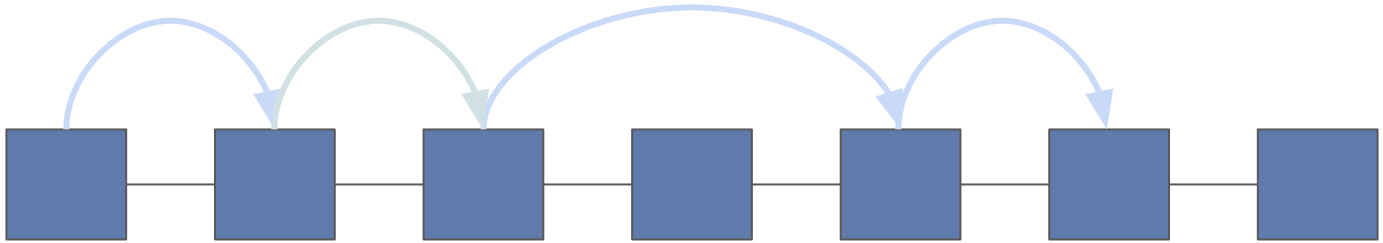
Finality gadget

- Leverage the security of the beacon chain to enhance the security of the existing proof-of-work chain

- Apply economic security from Casper protocol to Eth1.x
  - “finality”

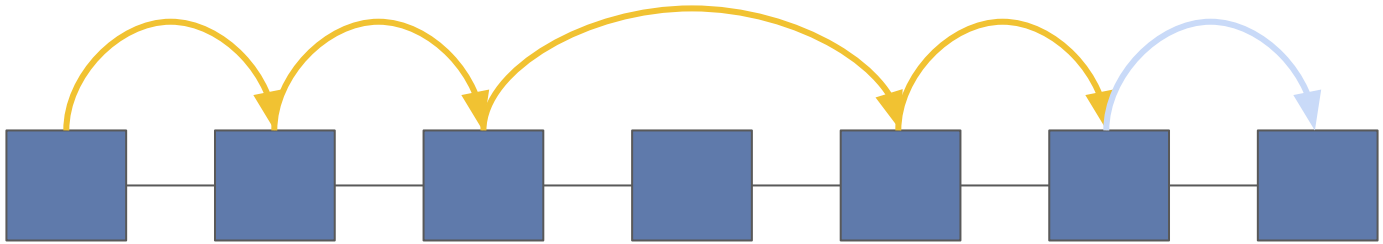
Finality

- In the normal case, validators attest to blocks in the canonical chain.



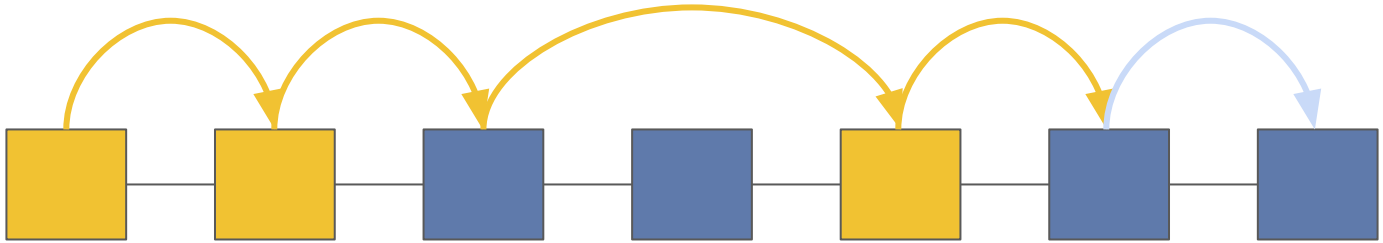
Finality

- If more than ⅔ of the validators attest to the a given block, it is justified.



Finality

- If the valiators make two successive justifications, then the first justified block is **finalized.**

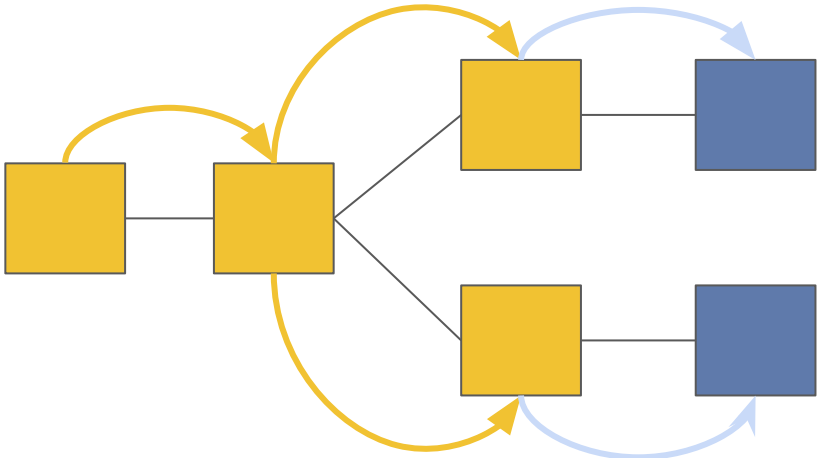


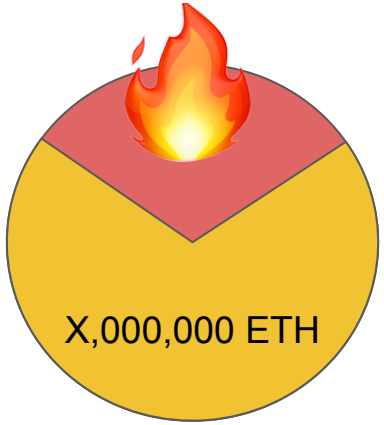
Why is “finality” final?

- Given the way Casper is constructed, if a block becomes finalized we can *prove* that either

    1) No conflicting block has been finalized

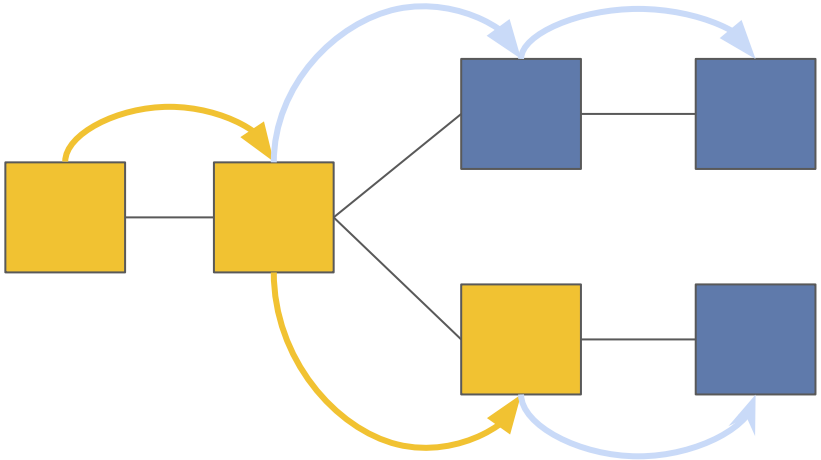
    2) At least ⅓ of the validators forfeited their funds at risk

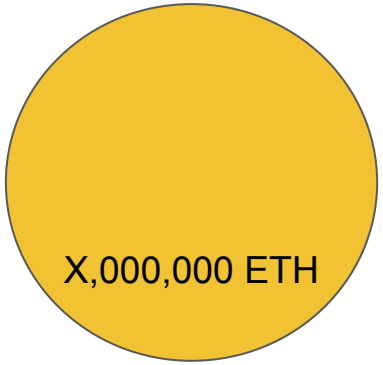




Why is “finality” final?

- Get a single, finalized chain

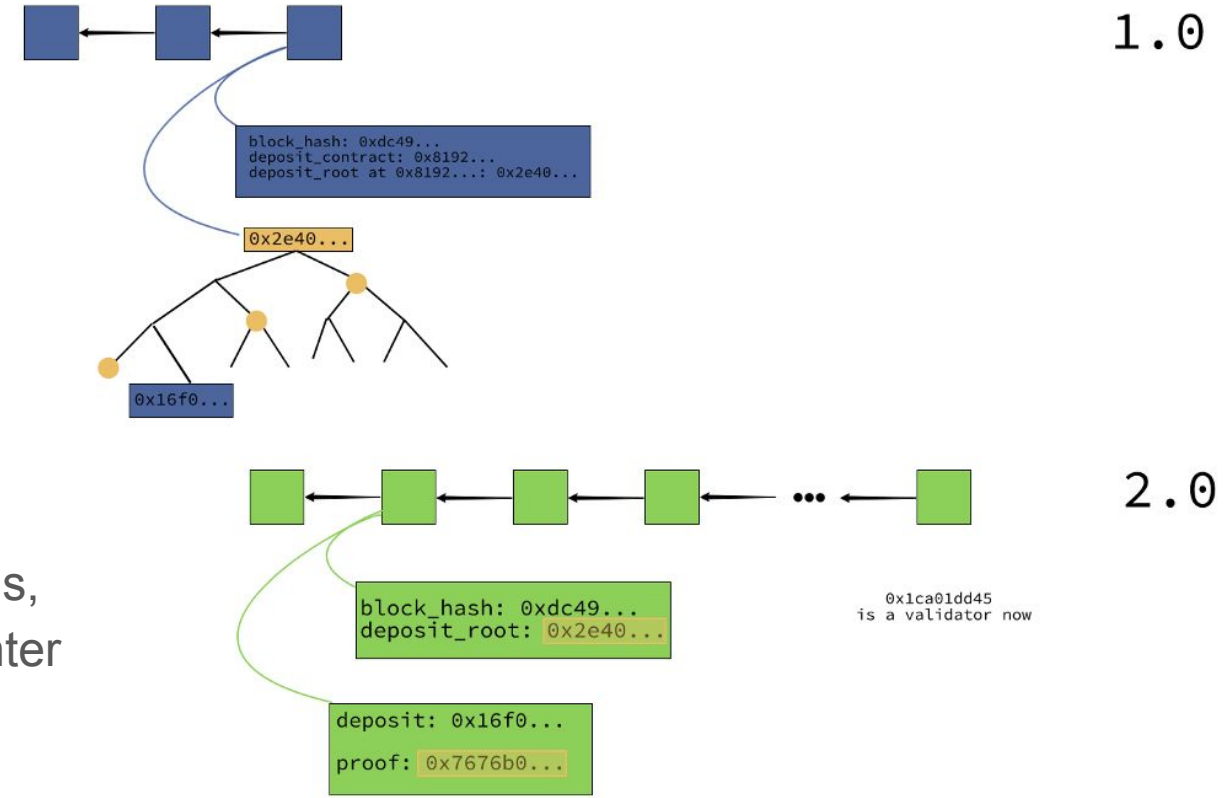




Finality example

- 10M ETH in beacon chain
- 3.3M ETH has to be burned under successful attack
- More than $700M to successfully attack

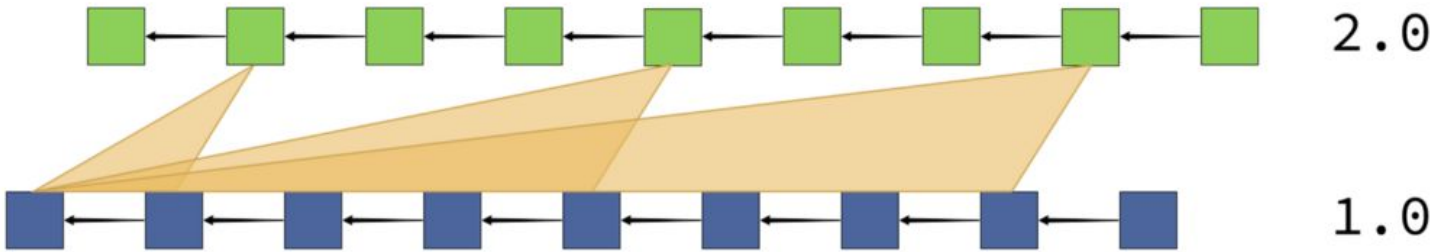
Finality gadget



- Under normal conditions, Eth1.0 block hashes enter the beacon chain with every beacon block

Finality gadget

- And, the Casper consensus *finalizes* these beacon blocks
- If an Eth1.0 block hash is finalized on the beacon chain, then every block beneath it in on the Eth1.0 chain is implicitly finalized as well



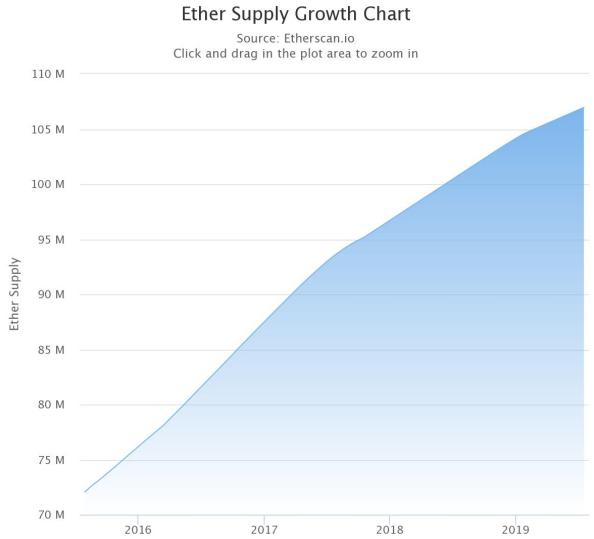
Why do we want it?

- Better security for proof-of-work chain
  - Can “fork out” malicious stake
  - For each single attack, “it is as if your ASIC farm burned down”
    - -- Vlad Zamfir

- Deterministic confirmations
  - No chance of a proof-of-work re-org attacking the chain
  - Gives better guarantees for some dApps
    - Lotteries, prediction markets, etc...

Why do we want it?, cont

- Can reduce overall ETH issuance
  - A blockchain should only make enough base token to purchase enough security
  - Reduce mining rewards as we all transition over to a proof-of-stake model
  - Should be able to make proof-of-stake issuance much lower than proof-of-work today



Why do we want it?

- Get tangible benefit out of eth2.0 soon
  - Way before phase 2!

eth1  eth2

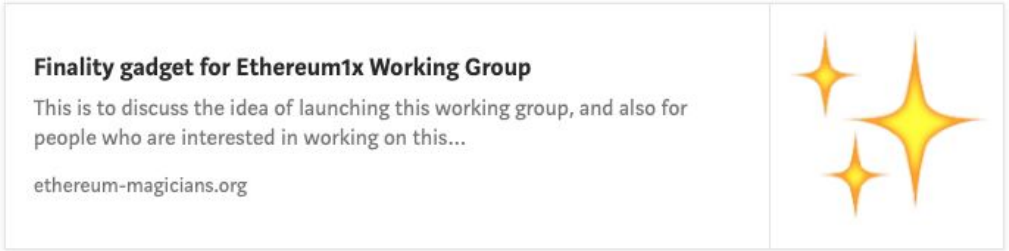
Risks, next steps

- A lot could go wrong
  - Coupling a new, untested system to one already in flight

- Can take a conservative approach to rolling it out
  - Simulations ⇦ we are here
  - EIP, community consensus
  - Deployment

Get involved!

- Ethereum 1.x Working Group
  - https://ethereum-magicians.org/t/finality-gadget-for-ethereum1x-working-group/3177



More info

- https://medium.com/@ralexstokes

- Feel free to reach out directly for more info, questions, etc.
  - @ralexstokes on Twitter, Telegram