# Cryptoeconomics in Casper

Jon Choi

@ Hashed Lounge. Seoul, Korea

December 12th, 2017

# Objectives

- Review why we’re working on Proof of Stake and Casper
- Share a few of the latest cryptoeconomic research

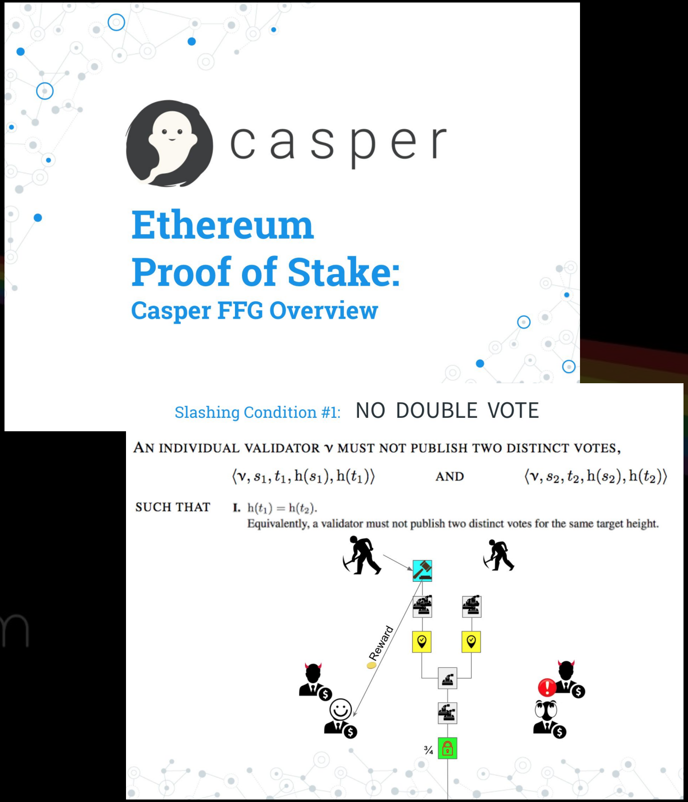
# Agenda

- **Proof of Stake & Casper 101** (15min) 👈🏼 🦄
- **Cryptoeconomics in Casper** (25 min)
  - Participation Constraint
  - CAPM & Sharpe Ratio
  - Validator Slashing Trilemma

# Casper implements proof of stake in Ethereum

# Rationale not implementation

- For implementation, refer to Karl's latest presentation about FFG deep dive.
- For the purposes of this presentation, we will focus on rationale for Casper and the cryptoeconomic optimizations.



casper

**Ethereum Proof of Stake:**

**Casper FFG Overview**

Slashing Condition #1: NO DOUBLE VOTE

AN INDIVIDUAL VALIDATOR $\nu$ MUST NOT PUBLISH TWO DISTINCT VOTES,

$\langle \nu, s_1, t_1, h(s_1), h(t_1) \rangle$ AND $\langle \nu, s_2, t_2, h(s_2), h(t_2) \rangle$

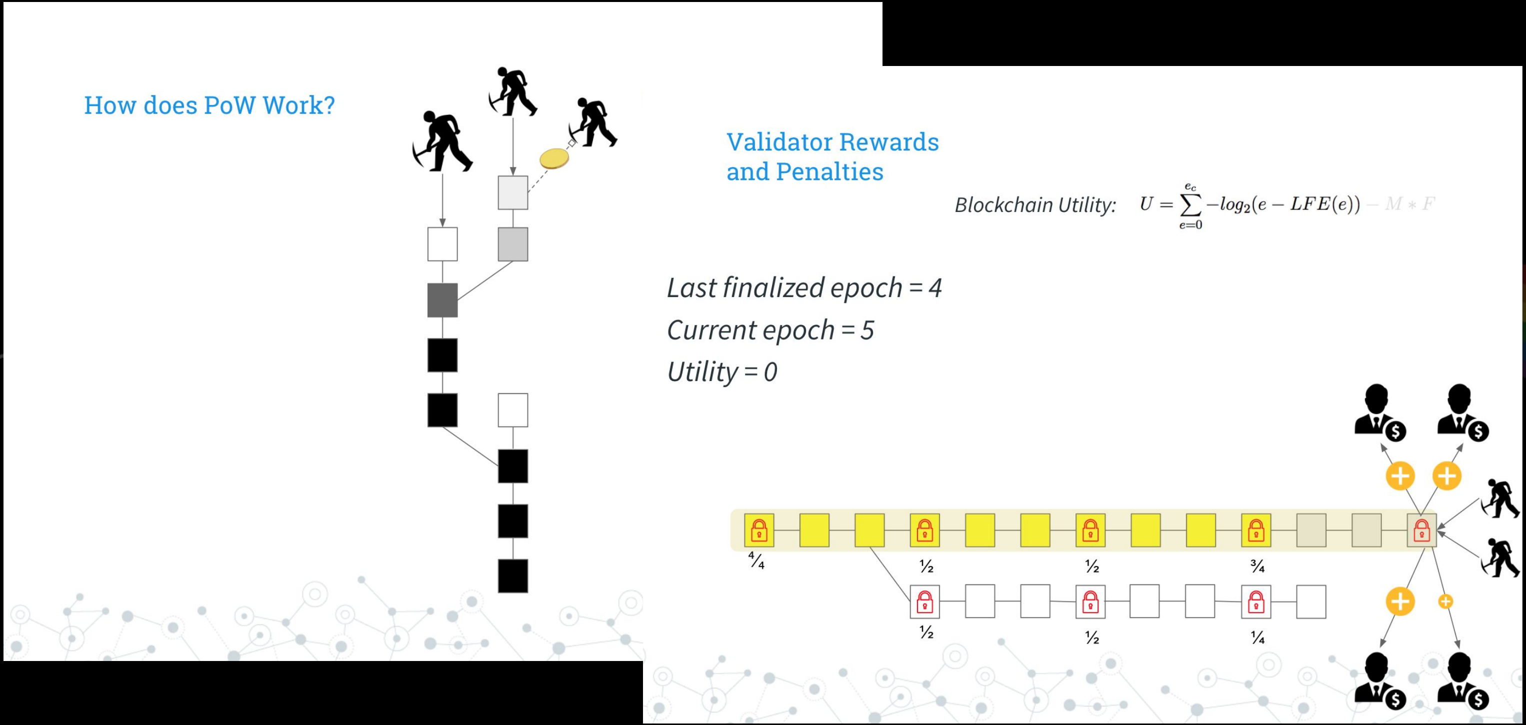
SUCH THAT I. $h(t_1) = h(t_2)$.
Equivalently, a validator must not publish two distinct votes for the same target height.

Credit: Karl Floersch

# FFG Brief Review

- Hybrid PoS/PoW. PoS overlay on top of existing PoW chain.
- Every 50 blocks is a checkpoint.
- 2/3 deposit-weighted votes constitutes a supermajority link.
- A supermajority link justifies the source epoch.
- Two consecutive supermajority links finalizes the second source epoch.
- Slashed if validator contradicts itself: double-vote, surround vote.
- Penalized if group fails to maintain safety & liveness.
- Otherwise, rewarded for securing the network.

# FFG Brief Review (cont.)



How does PoW Work?

Validator Rewards and Penalties

Blockchain Utility: $U = \sum_{e=0}^{e_c} -log_2(e - LFE(e)) - M * F$

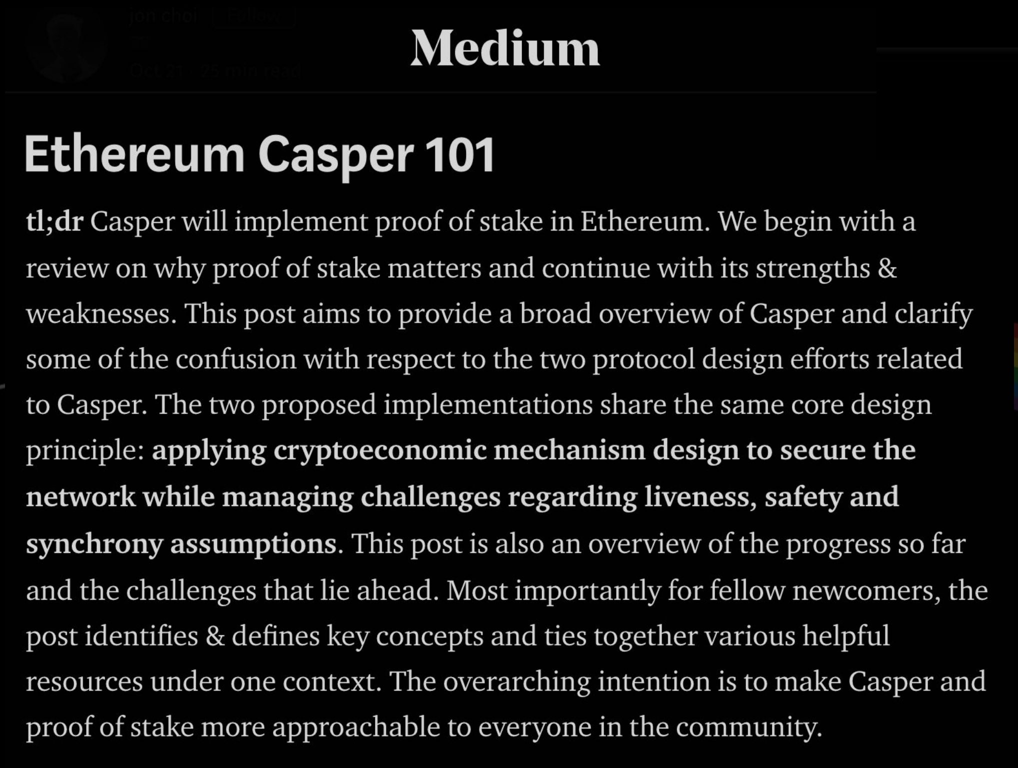
*Last finalized epoch = 4*

*Current epoch = 5*

*Utility = 0*

Credit: Karl Floersch

# Medium



jon choi

Oct 21 · 25 min read

## Ethereum Casper 101

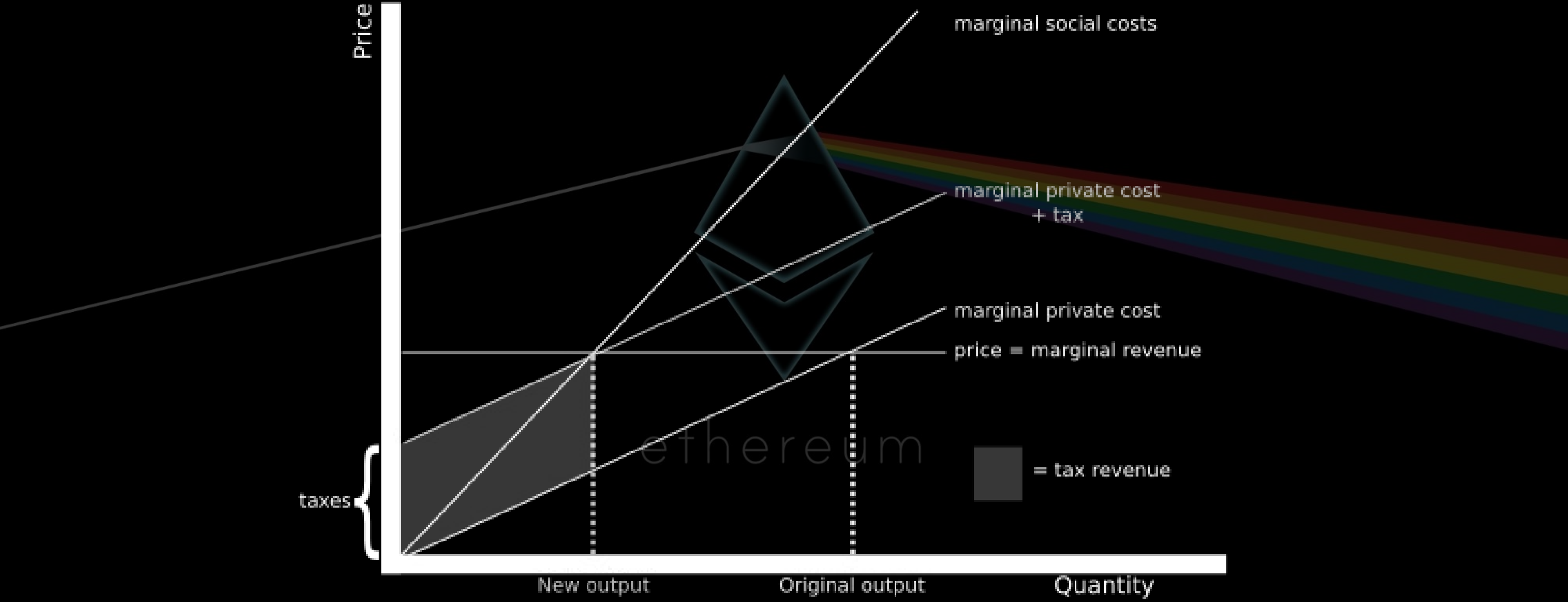
**tl;dr** Casper will implement proof of stake in Ethereum. We begin with a review on why proof of stake matters and continue with its strengths & weaknesses. This post aims to provide a broad overview of Casper and clarify some of the confusion with respect to the two protocol design efforts related to Casper. The two proposed implementations share the same core design principle: **applying cryptoeconomic mechanism design to secure the network while managing challenges regarding liveness, safety and synchrony assumptions**. This post is also an overview of the progress so far and the challenges that lie ahead. Most importantly for fellow newcomers, the post identifies & defines key concepts and ties together various helpful resources under one context. The overarching intention is to make Casper and proof of stake more approachable to everyone in the community.

# Review: Proof of Stake

# Energy Efficiency, Decentralization, & Mechanism Design

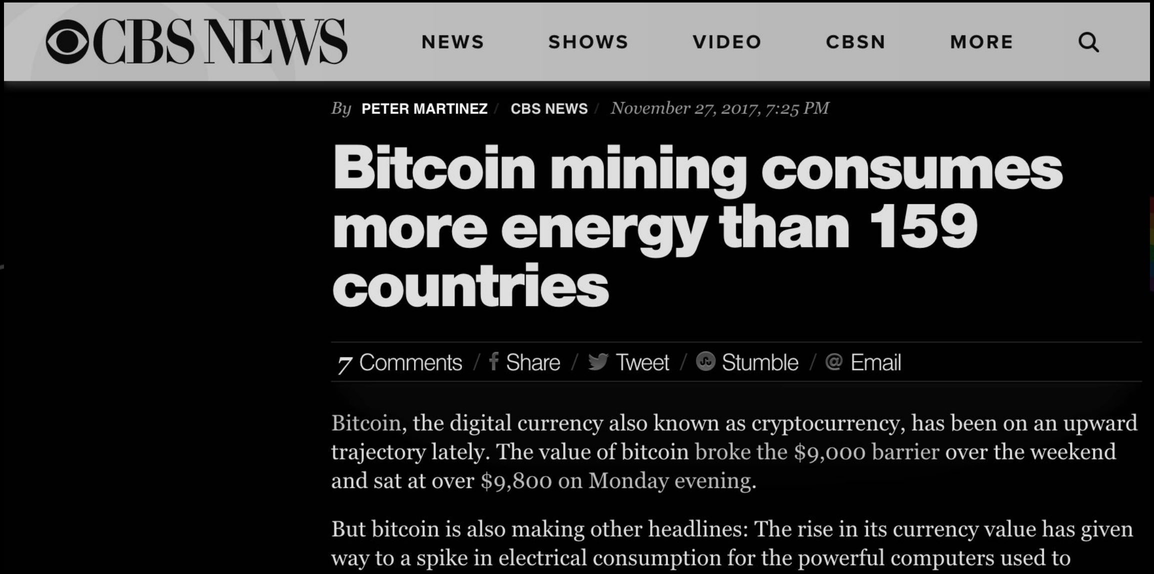
# 1. Energy Efficiency

# Econ Detour: Public vs Private Cost/Benefit



Credit: Wikimedia

# Already non-trivial energy wastage...



By PETER MARTINEZ / CBS NEWS / November 27, 2017, 7:25 PM

## Bitcoin mining consumes more energy than 159 countries

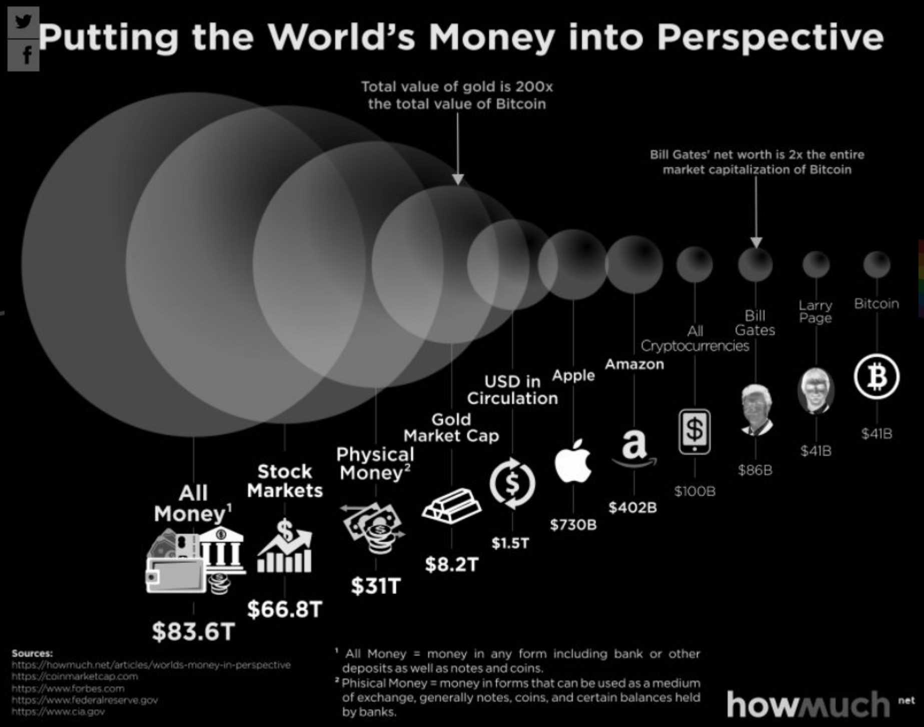
7 Comments / Share / Tweet / Stumble / Email

Bitcoin, the digital currency also known as cryptocurrency, has been on an upward trajectory lately. The value of bitcoin broke the $9,000 barrier over the weekend and sat at over $9,800 on Monday evening.

But bitcoin is also making other headlines: The rise in its currency value has given way to a spike in electrical consumption for the powerful computers used to

Credit: CBS

# … and cryptocurrencies have a long way to go.



Credit: How much / Business Insider

If cryptocurrencies achieve the full vision,
PoW will require much more wasted energy.

# Counterargument: social scalability?

> “Reverse-engineering our highly evolved traditional institutions … will usually work better than designing from scratch, than grand planning and game theory.
>
> …sacrifice computational efficiency and scalability--consume more cheap computational resources--in order to reduce and better leverage the great expense in human resources needed to maintain the relationships between strangers involved modern institutions such as markets, large firms, and governments.”
>
> – Nick Szabo, Unenumerated

Goal: achieve social scalability with less environmental cost.

# Social scalability with less realized cost

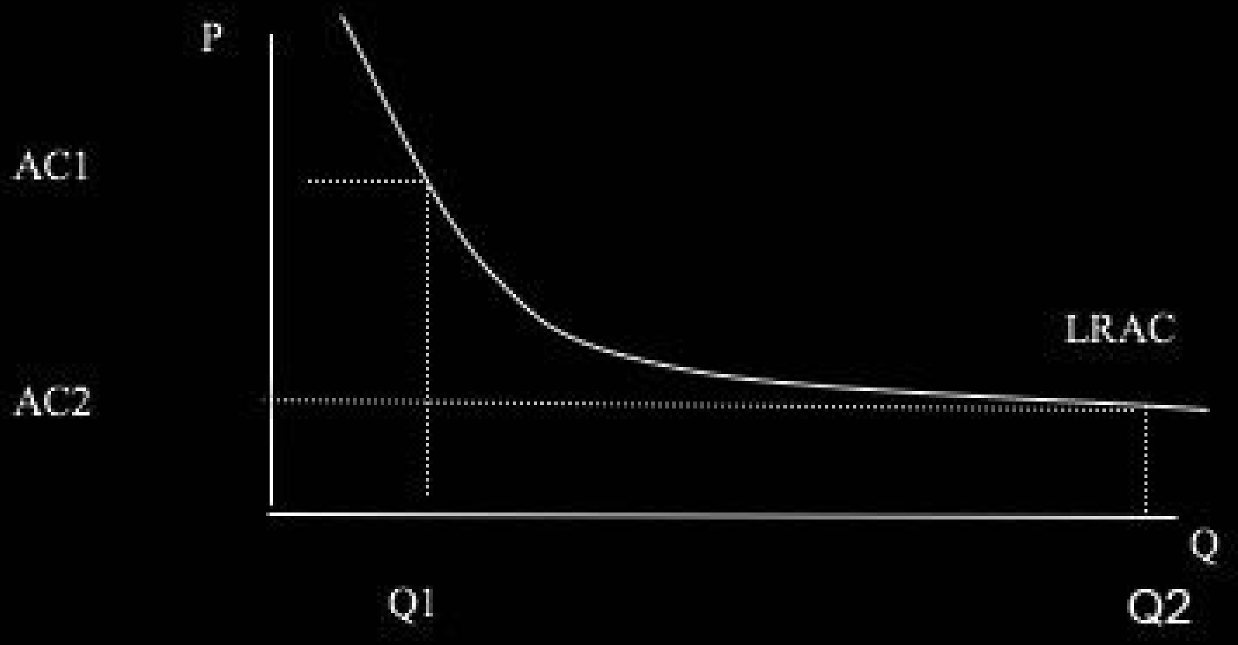
- Example: Public Transit Ticketing
  - Realized cost: Have everyone take 2 minutes to load their transit card and pay per trip.
  - Risk of Loss: Honor system, but if you're caught without a ticket, you get a fine that's worth a 100 trips.
- Social Scaling: better global outcome to pool taxes and create a centrally planned infrastructure than for everyone to commute in cars.

# Energy Efficiency:

Incentivizing with realized costs vs risk of loss.

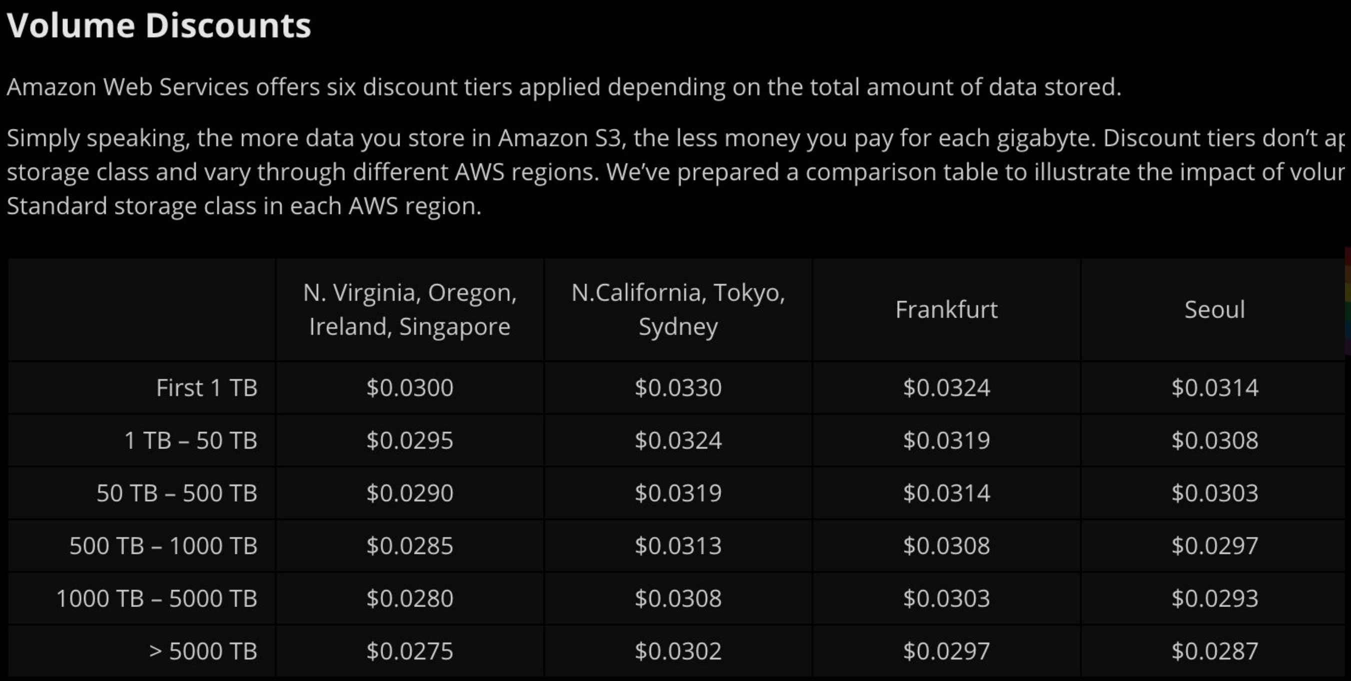
# 2. Decentralization

# Econ Detour: Mitigate Economies of Scale



Credit: economicshelp.org

# Economies of Scale: AWS



## Volume Discounts

Amazon Web Services offers six discount tiers applied depending on the total amount of data stored.

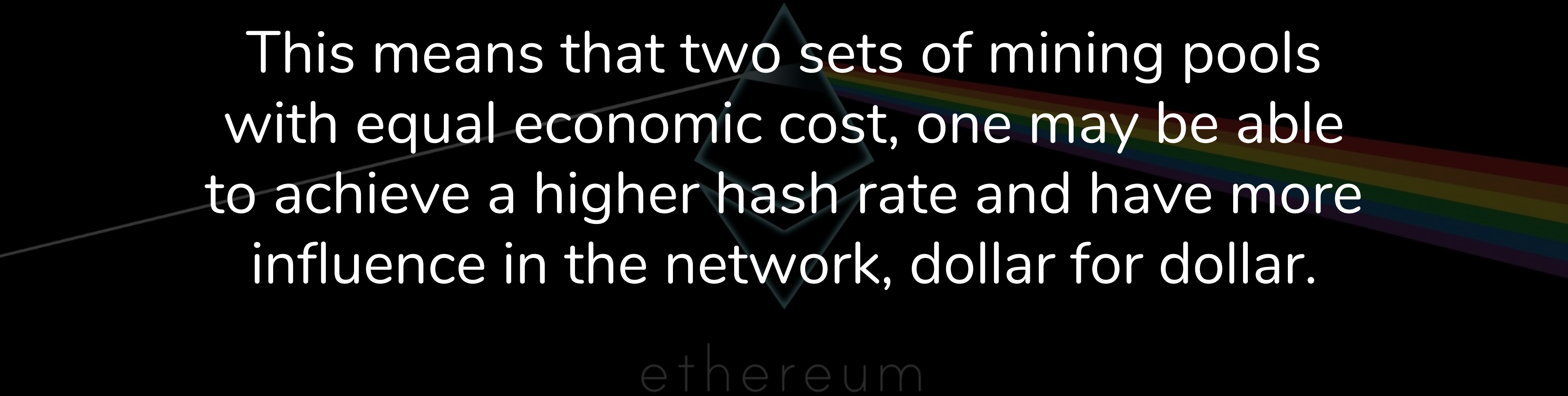
Simply speaking, the more data you store in Amazon S3, the less money you pay for each gigabyte. Discount tiers don't ap
storage class and vary through different AWS regions. We've prepared a comparison table to illustrate the impact of volur
Standard storage class in each AWS region.

| | N. Virginia, Oregon, Ireland, Singapore | N.California, Tokyo, Sydney | Frankfurt | Seoul |
|---|---|---|---|---|
| First 1 TB | $0.0300 | $0.0330 | $0.0324 | $0.0314 |
| 1 TB – 50 TB | $0.0295 | $0.0324 | $0.0319 | $0.0308 |
| 50 TB – 500 TB | $0.0290 | $0.0319 | $0.0314 | $0.0303 |
| 500 TB – 1000 TB | $0.0285 | $0.0313 | $0.0308 | $0.0297 |
| 1000 TB – 5000 TB | $0.0280 | $0.0308 | $0.0303 | $0.0293 |
| > 5000 TB | $0.0275 | $0.0302 | $0.0297 | $0.0287 |

Credit: AWS

# Mitigation of Centralization

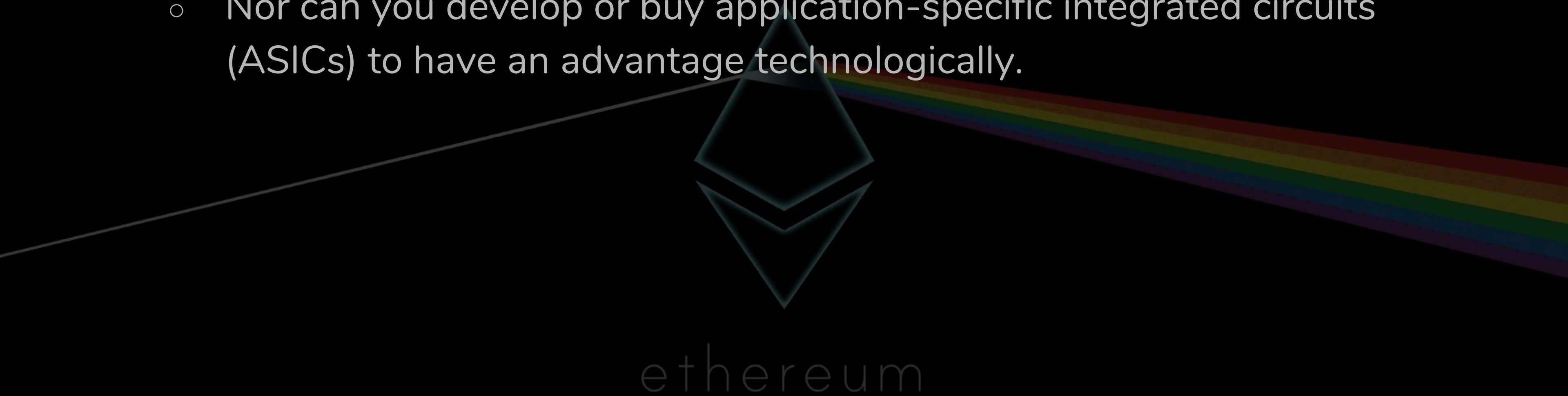
- Proof of work mining pools can lower the unit cost of their infrastructure (datacenter costs, power costs, personnel)
  - (1) amortizing a fixed cost over a larger operation
  - (2) having bargaining power by operating as a larger entity.
- Examples:
  - Lower $/sqft for datacenter space
  - Lower $/kwh for larger/longer lease
  - Lower headcount cost / GH
  - Negotiating cheaper cost for ASICs and other equipment for buying in volume.



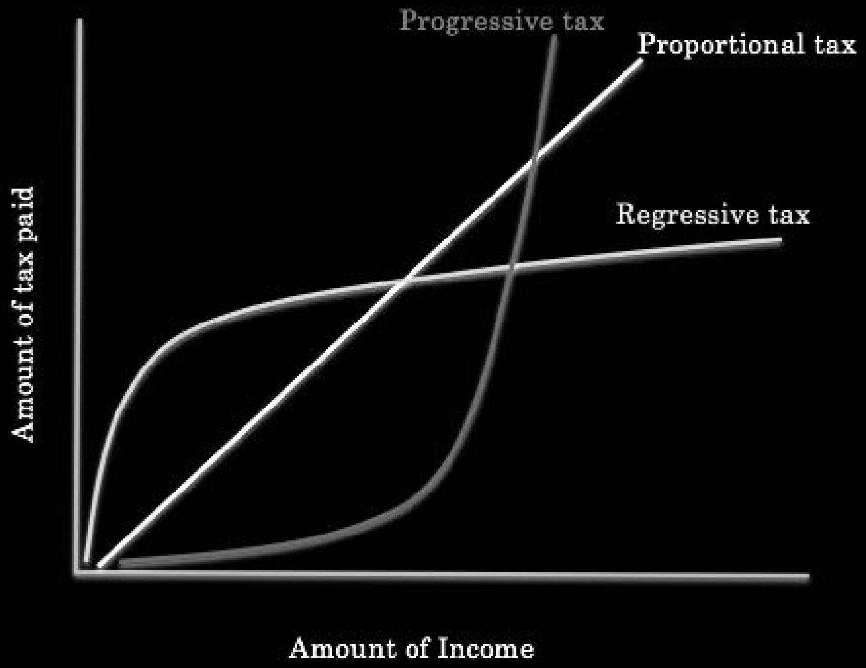
This means that two sets of mining pools with equal economic cost, one may be able to achieve a higher hash rate and have more influence in the network, dollar for dollar.

# “Dollar is a Dollar”

- The benefit here is that you can’t pool together to make a dollar worth more.
  - Nor can you develop or buy application-specific integrated circuits (ASICs) to have an advantage technologically.



# Econ Detour: Inequality and Scale



Credit: Google Images

# Regressive to ~Proportional

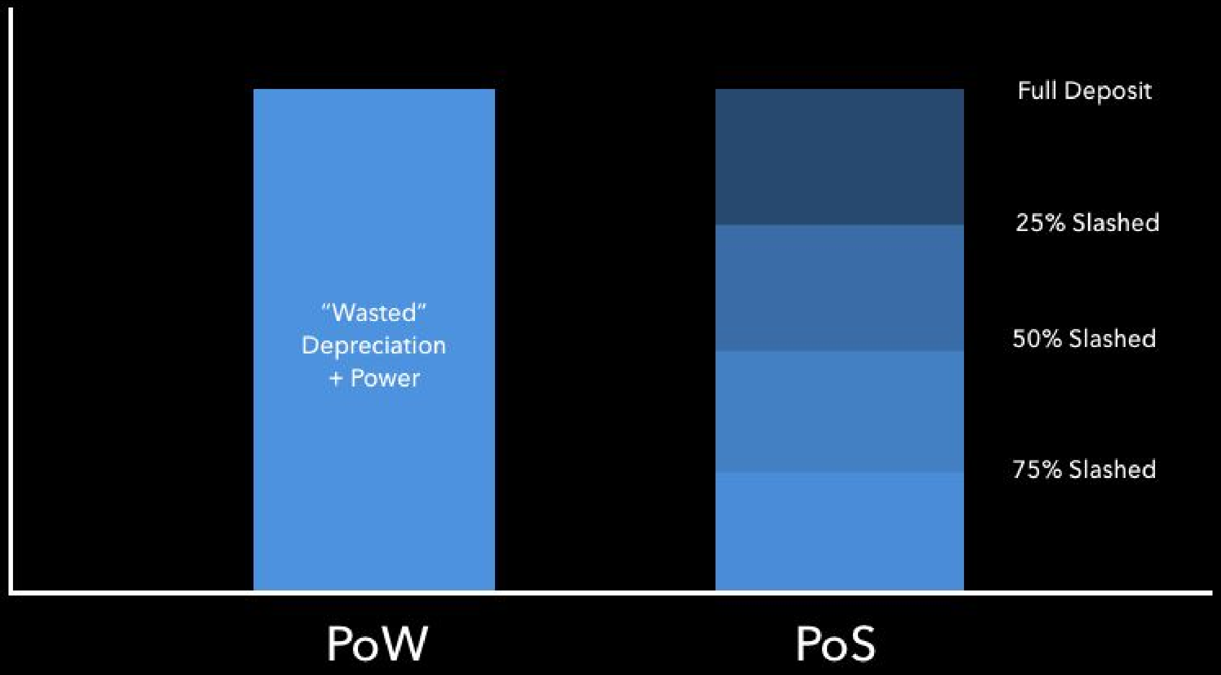
- So, PoS intends to mitigate the regressive distribution of PoW mining rewards and move directionally towards proportional distribution.
- Going beyond proportional to progressive distribution will require mature decentralized reputation/identity management services to prevent larger validators splitting themselves into many smaller validators.

# Decentralization:

# Diminish economies of scale

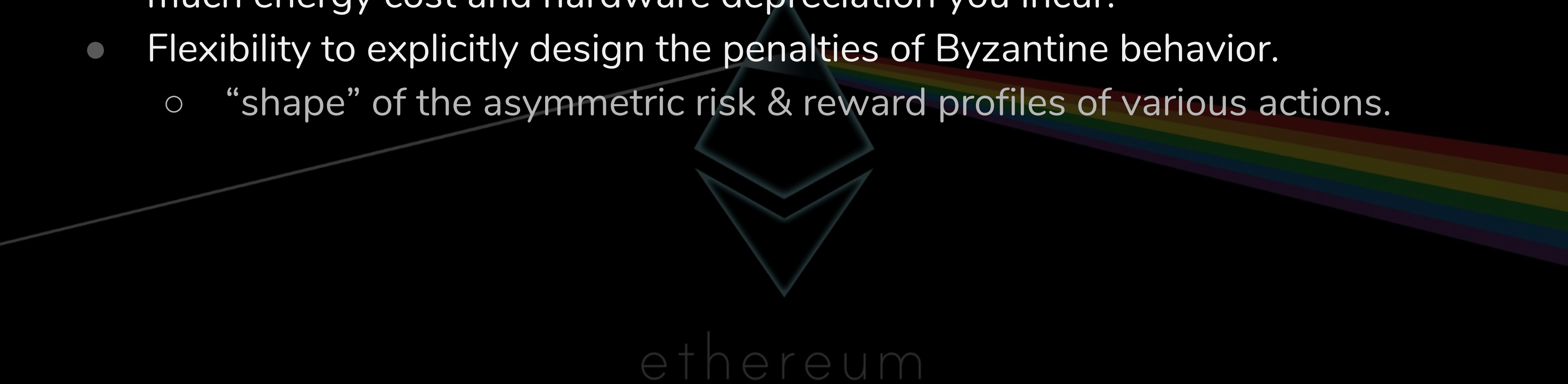
# 3. More Flexible Mechanism Design

# Explicit Control over Penalty



# Explicit Economic Security

- **As opposed to what?** In PoW, your downside is implicitly capped at how much energy cost and hardware depreciation you incur.
- Flexibility to explicitly design the penalties of Byzantine behavior.
  - “shape” of the asymmetric risk & reward profiles of various actions.



PoS may be more challenging to design, but it allows for much more fine-grained control over the rewards and penalties.

We will talk more about this later in the talk.

## Why Casper Matters

Now that we have decoded what this mysterious Casper project is. Let's synthesize what we learned about PoS and Casper to understand why this matters.

In simple terms:

1. Decentralization (*covered in PoS*)
2. Energy efficiency (*covered in PoS*)
3. Explicit Economic Security (*covered in PoS*)
4. Scaling Ethereum
5. Gentle Transition from PoW

# Stepping Stone to Pure PoS

# Gentle Transition

- Plan for PoS since 2014
- FFG is on-ramp to PoS
- ETH is $40B+ network. Moving slowly.

# Finality & Scaling

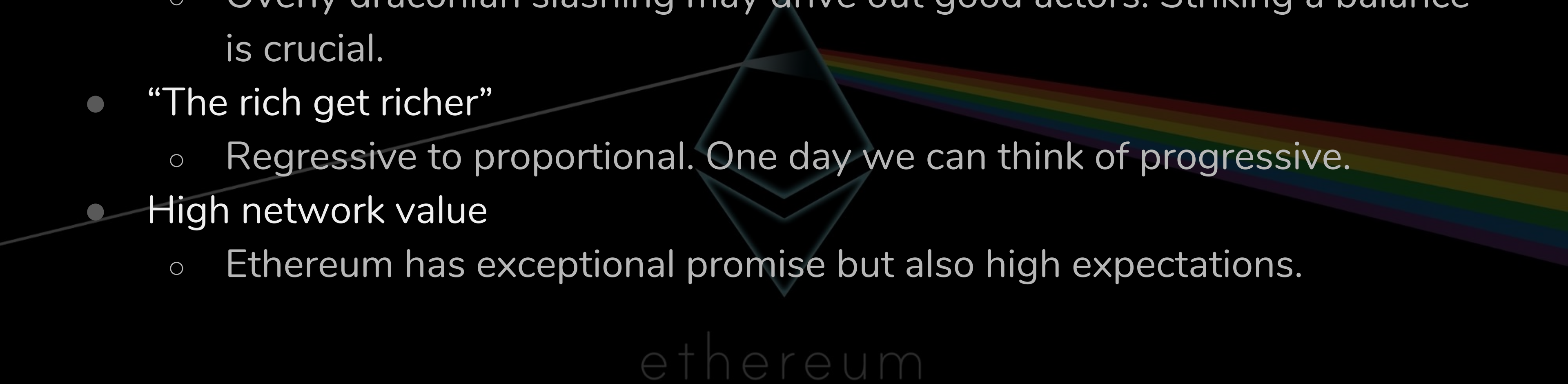
# Casper & Scaling

- Explicit finality, as opposed to probabilistic finality
- Security in sharding

# Scale, not speed.

- Scaling beyond 10 tx/s
- Faster applications via state channels and plasma
- Finality helps each shard maintain security
- Analogy: not finalizing your coffee tx, letting the network handle more coffee txs per block time.

# Challenges



- Adverse selection
  - Overly draconian slashing may drive out good actors. Striking a balance is crucial.
- “The rich get richer”
  - Regressive to proportional. One day we can think of progressive.
- High network value
  - Ethereum has exceptional promise but also high expectations.

# FFG vs TFG

# A Tale of Two Caspers

- Not a specific implementation but a family of two main projects under active research
- The Friendly Finality Gadget (“FFG”)—aka “Vitalik’s Casper”—is a hybrid PoW/PoS consensus mechanism
- Casper the Friendly GHOST (“TFG”)—aka “Vlad’s Casper”—is a pure PoS proof of concept and will inform future iterations

# Shared Casper Design Principles

1. Economics to design behavior.
2. Maximize cost of attack.
3. Public cost-benefit, not just private.
4. Prevent economies of scale.
5. Network security is derived from “skin in the game.”
6. Design for oligopolies.
7. Accountable safety.
8. Decentralized things should be able to regenerate.
9. Disincentivize censorship.
10. ...more in Casper 101

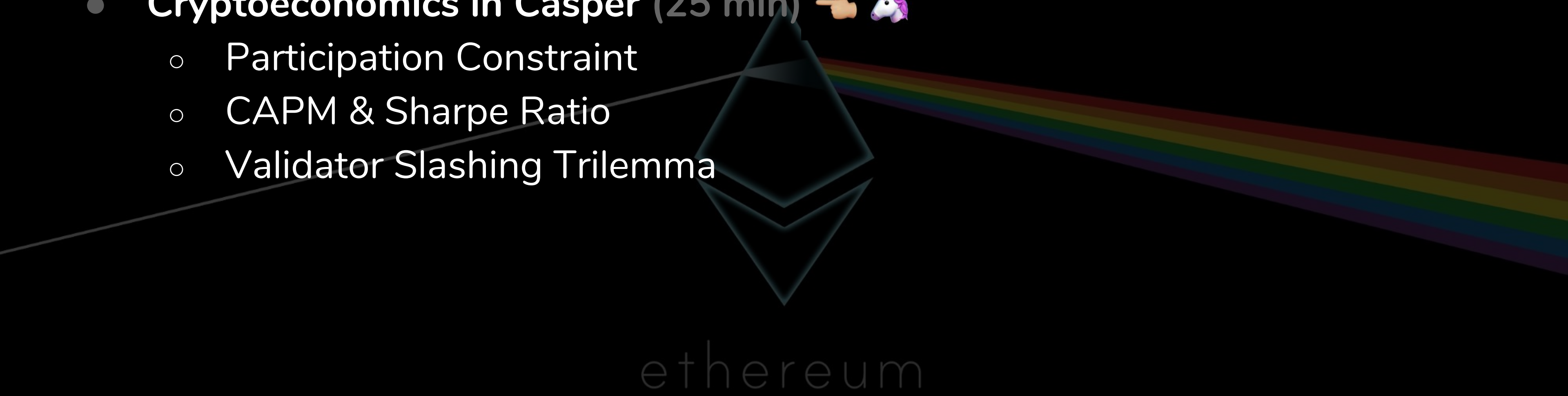
# Shared Casper Design Principles

1. Economics to design behavior.
2. Maximize cost of attack.
3. Public cost-benefit, not just private.
4. Prevent economies of scale.
5. Network security is derived from “skin in the game.”
6. Design for oligopolies.
7. Accountable safety.
8. Decentralized things should be able to regenerate.
9. Disincentivize censorship.
10. ...more in Casper 101

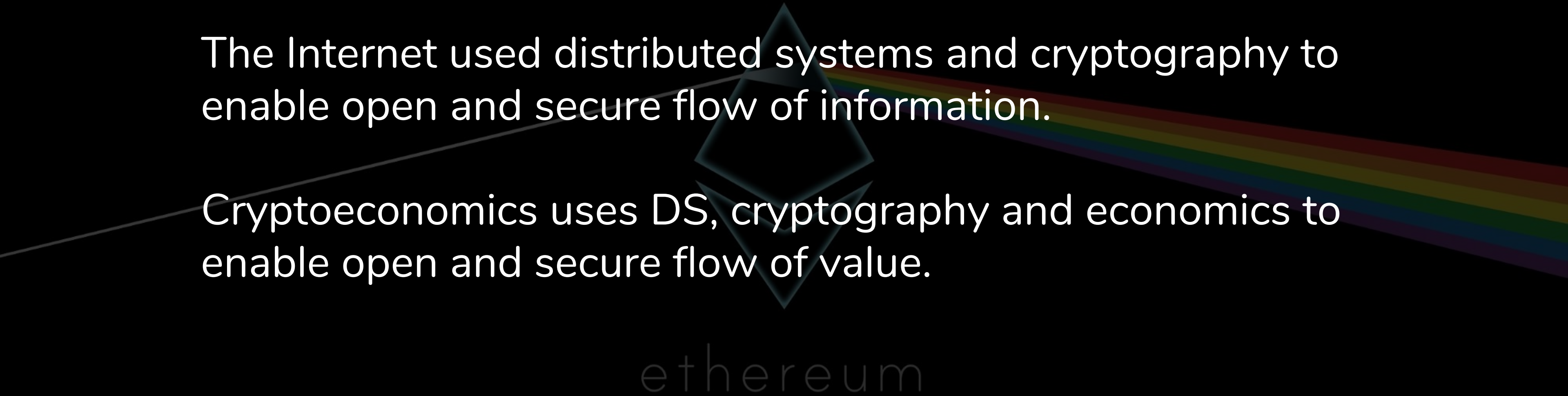
Cryptoeconomics

# Agenda

- **Proof of Stake & Casper 101** **(15min)**
- **Cryptoeconomics in Casper** **(25 min)** 👉🏼 🦄
  - Participation Constraint
  - CAPM & Sharpe Ratio
  - Validator Slashing Trilemma



# Why does cryptoeconomics matter?



The Internet used distributed systems and cryptography to enable open and secure flow of information.

Cryptoeconomics uses DS, cryptography and economics to enable open and secure flow of value.

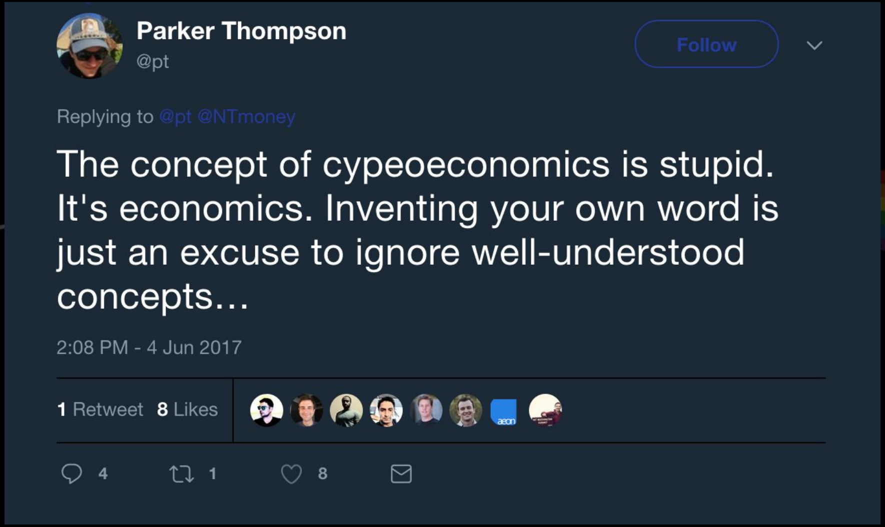
The Internet enabled Google, Facebook, Amazon, Apple to connect the world–under their third-party custody.

Blockchains can enable connecting the world–under the custody of the participants.

While the ethos is powerful, the mechanisms need to succeed in incentivizing intended behavior in order to achieve the vision.

# So, what is cryptoeconomics?

# Why bother defining it?



**Parker Thompson**
@pt

Replying to @pt @NTmoney

The concept of cypeoeconomics is stupid. It's economics. Inventing your own word is just an excuse to ignore well-understood concepts…

2:08 PM - 4 Jun 2017

**1** Retweet **8** Likes

4 1 8

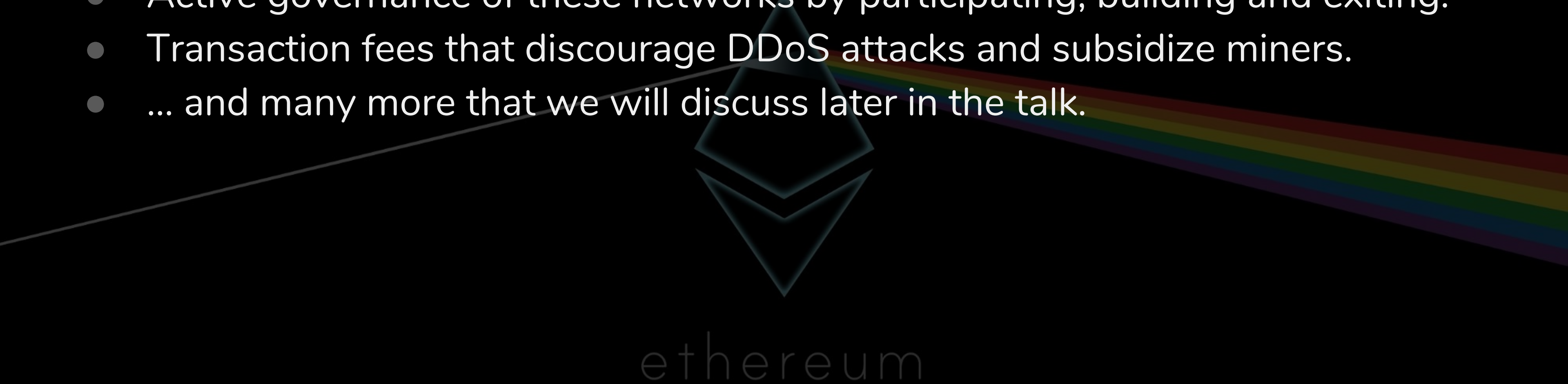
Cryptoeconomics is inherently multidisciplinary and it is necessarily a subfield of distributed systems, cryptography, microeconomics and macroeconomics.

**Cryptoeconomics** *noun*

The study of the use of incentives to achieve information security objectives.

# Examples of Cryptoeconomics

- Global network of miners that voluntarily secure the distributed ledger.
- Active governance of these networks by participating, building and exiting.
- Transaction fees that discourage DDoS attacks and subsidize miners.
- … and many more that we will discuss later in the talk.



# Latest Research

# Economic Research Objectives

- Penalize bad behavior and limit the damage it can do
  - Slashing, griefing factor, ulterior factor
- Reward good behavior
  - Voting frequently & correctly, reward cooperation
- Design a economically sound system and mechanism
  - Limit the dilution to existing ETH holders
  - High TD / MCap Ratio
  - Encourage broad participation (lower p_byzantine)

# Economic Research Areas

- Participation Constraint Analysis 👈🏼 🦄
- Sharpe Ratio and Perceived Risk/Reward Ratio
- Validator Slashing Trilemma

# What’s our budget?

# Quantity Theory of Money

$$M \cdot V_T = \sum_i (p_i \cdot q_i) = \mathbf{p}^{\mathrm{T}}\mathbf{q}$$

M = Money Supply

V = Velocity of Money

M * V = Total Spend

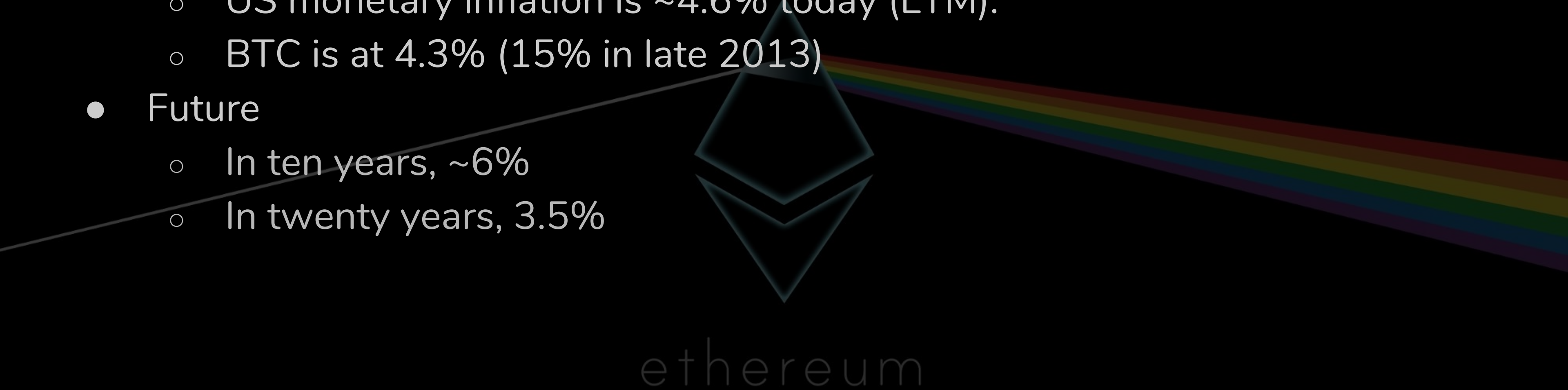
P = Price level

Q = Quantity of goods & services

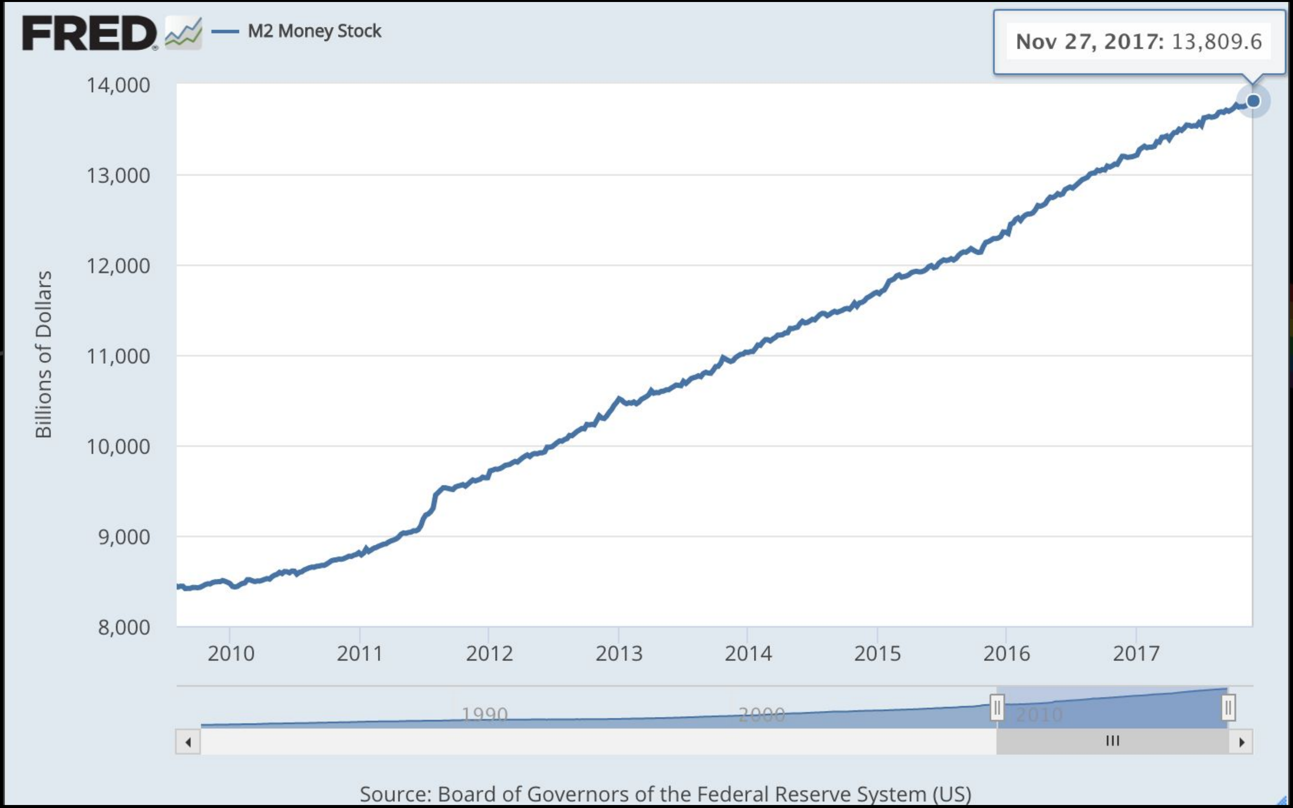
Credit: Wikipedia

# Monetary Inflation

- 2017 ETH monetary inflation on target for ~15%
  - US monetary inflation is ~4.6% today (LTM).
  - BTC is at 4.3% (15% in late 2013)
- Future
  - In ten years, ~6%
  - In twenty years, 3.5%

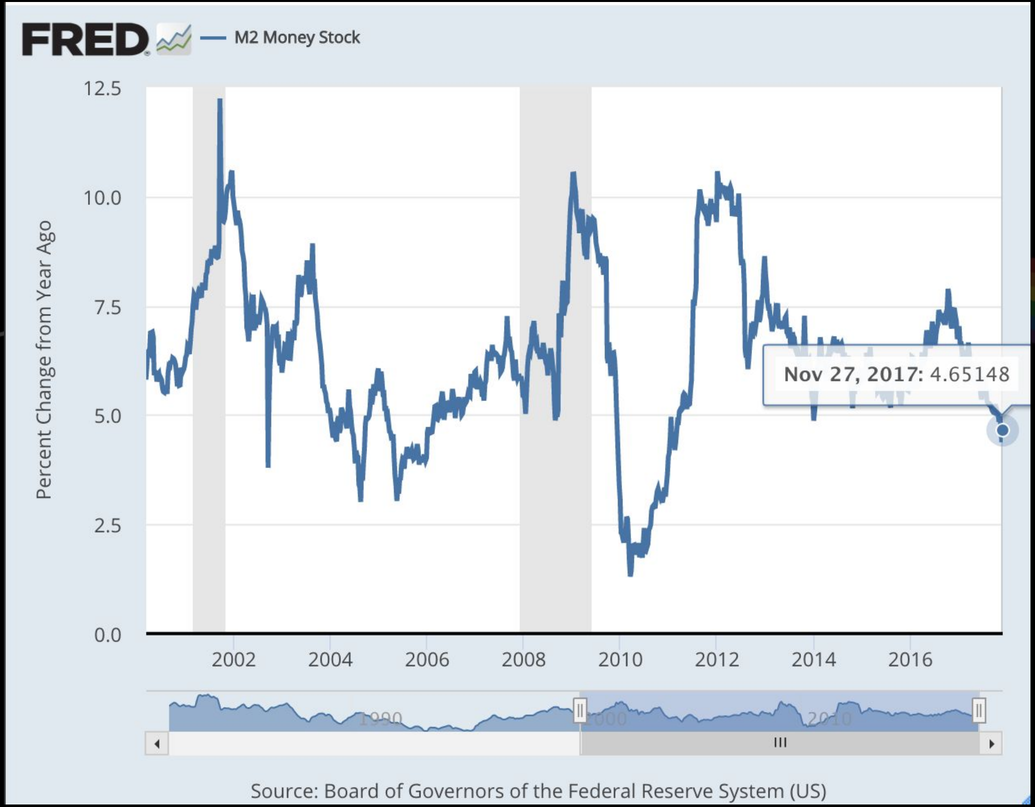


# Monetary Inflation



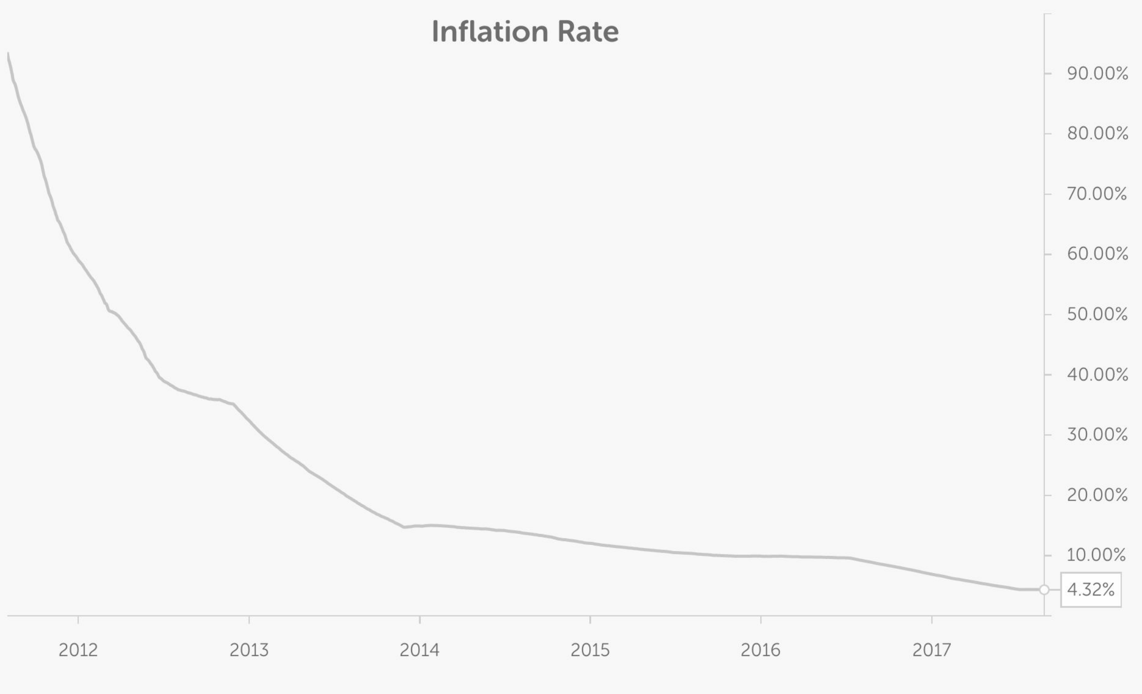
Source: Board of Governors of the Federal Reserve System (US)

# Monetary Inflation



Source: Board of Governors of the Federal Reserve System (US)

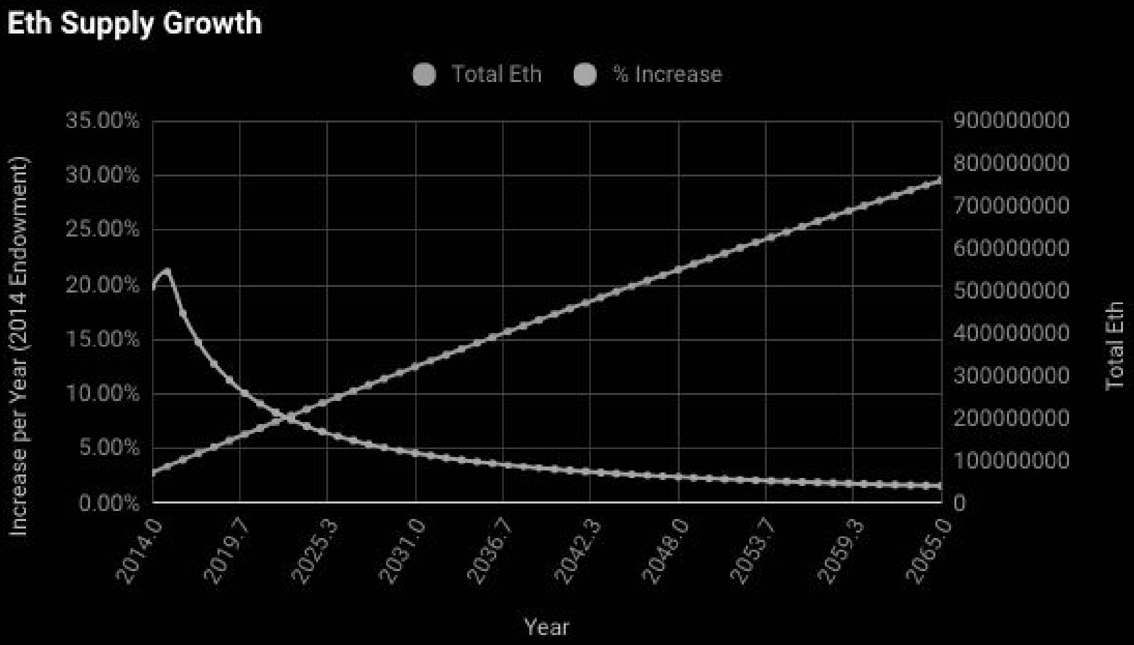
# How about for Bitcoin?



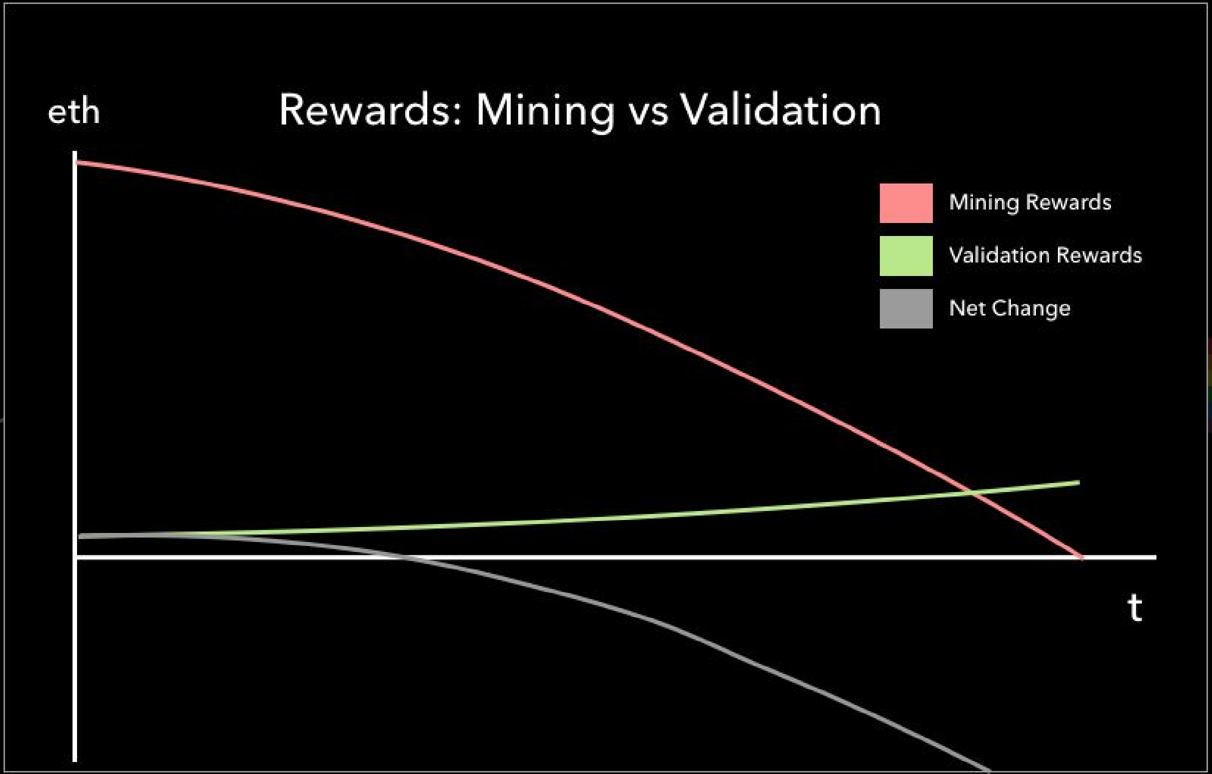
Credit: Bitcoin.com

# Ethereum Inflation Rate

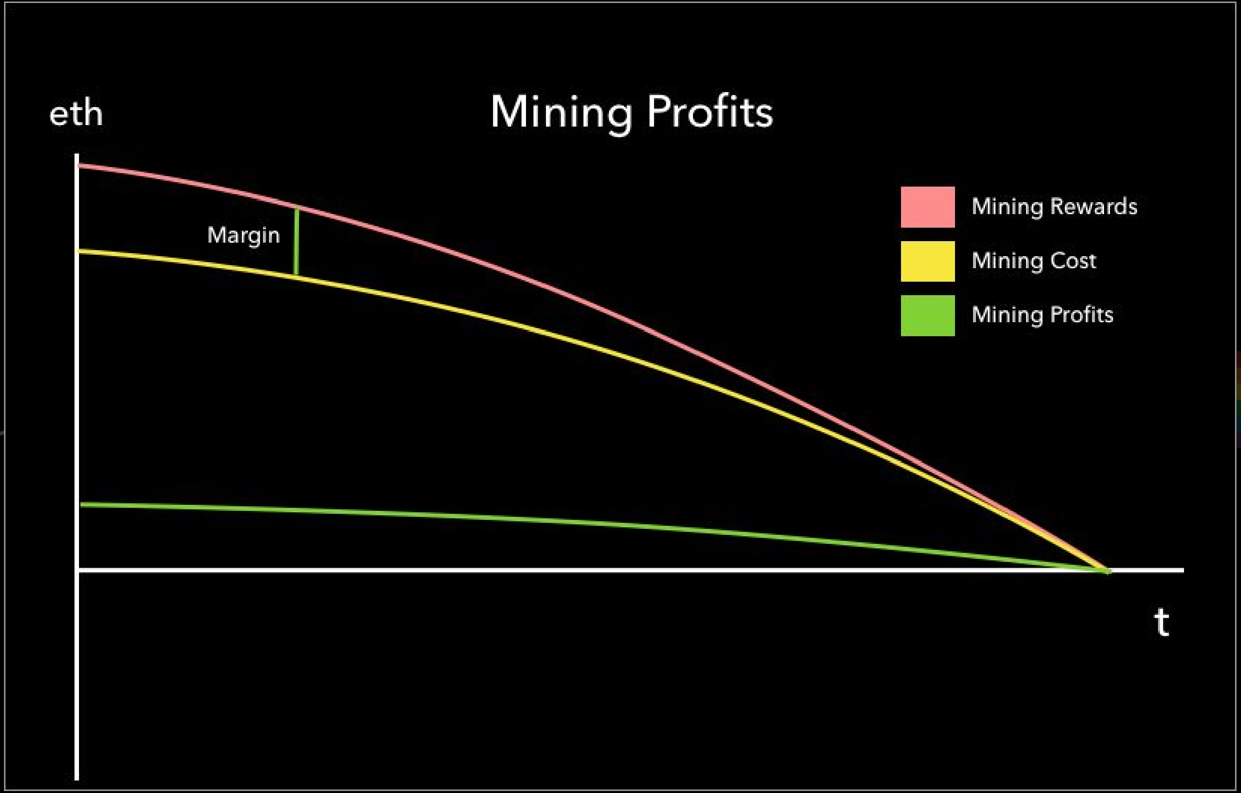
Validation will add to this. But Mining rewards will also go down over time.



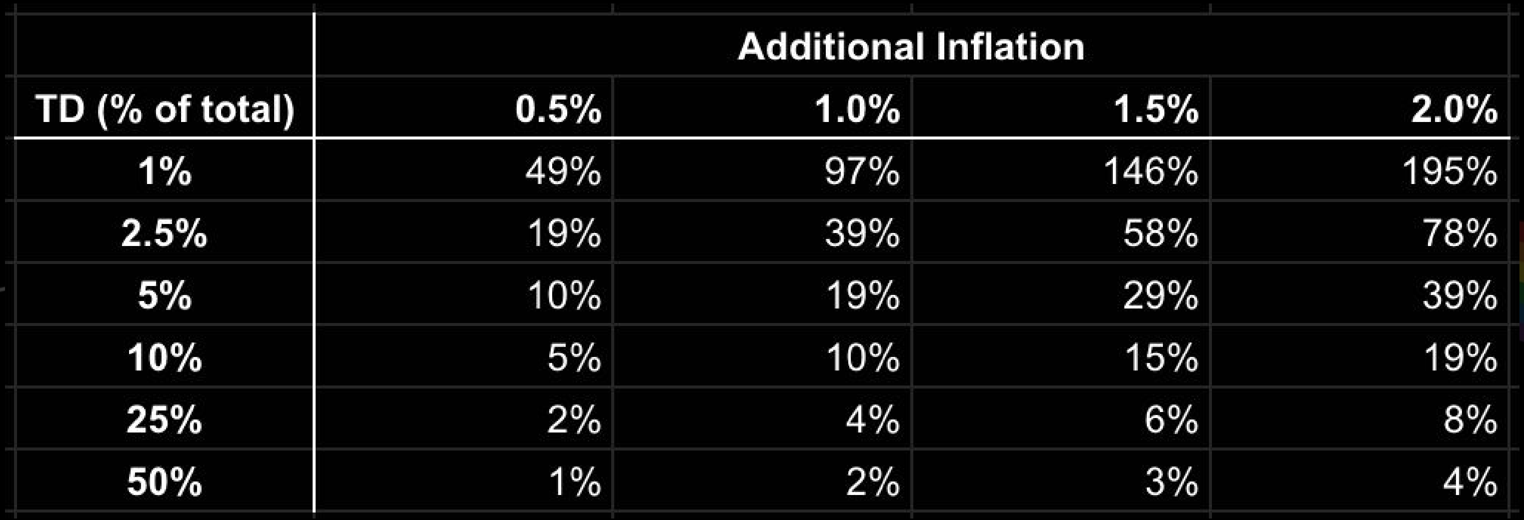
Credit: Joseph Lubin blogpost



Rewards: Mining vs Validation

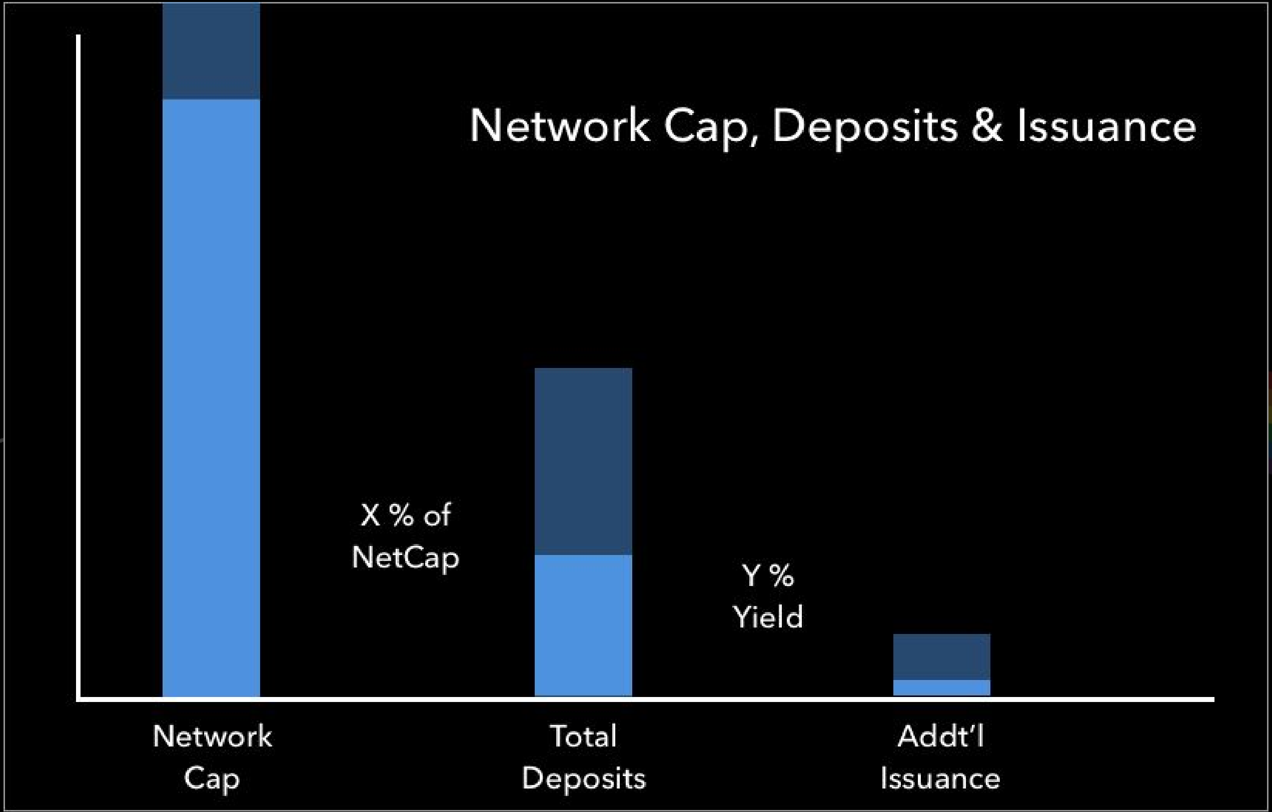

eth
Mining Profits
Margin
Mining Rewards
Mining Cost
Mining Profits
t

# Illustrative Validator Yield Ranges



| | Additional Inflation | | | |
|---|---|---|---|---|
| **TD (% of total)** | **0.5%** | **1.0%** | **1.5%** | **2.0%** |
| **1%** | 49% | 97% | 146% | 195% |
| **2.5%** | 19% | 39% | 58% | 78% |
| **5%** | 10% | 19% | 29% | 39% |
| **10%** | 5% | 10% | 15% | 19% |
| **25%** | 2% | 4% | 6% | 8% |
| **50%** | 1% | 2% | 3% | 4% |

Early research. Purely illustrative.


Network Cap, Deposits & Issuance
X % of NetCap
Y % Yield
Network Cap
Total Deposits
Addt'l Issuance

# Illustrative Analogies

- Nations
  - Central banking & monetary policy
    - Open Market Operations
- Companies
  - Corporate share buybacks
  - Capital raising Issuance

# Economic Research Areas

- Participation Constraint Analysis
- Sharpe Ratio and Perceived Risk/Reward Ratio 👈🏼 🦄
- Validator Slashing Trilemma

# Will people choose to participate?

# Participation Constraint Analysis

- “Will the mechanism be compelling enough for various validators to participate at all?”
    - Assuming that people will participate no matter what because “Ethereum is so great” is not acceptable
- Main Tradeoff: Issuance and average returns
- Design Consideration: Clearly communicating honest vs byzantine returns

# Risk Return Analysis

- CAPM & Sharpe Ratio
- “PRR” Ratio

Credit: Prentice Hall 2008

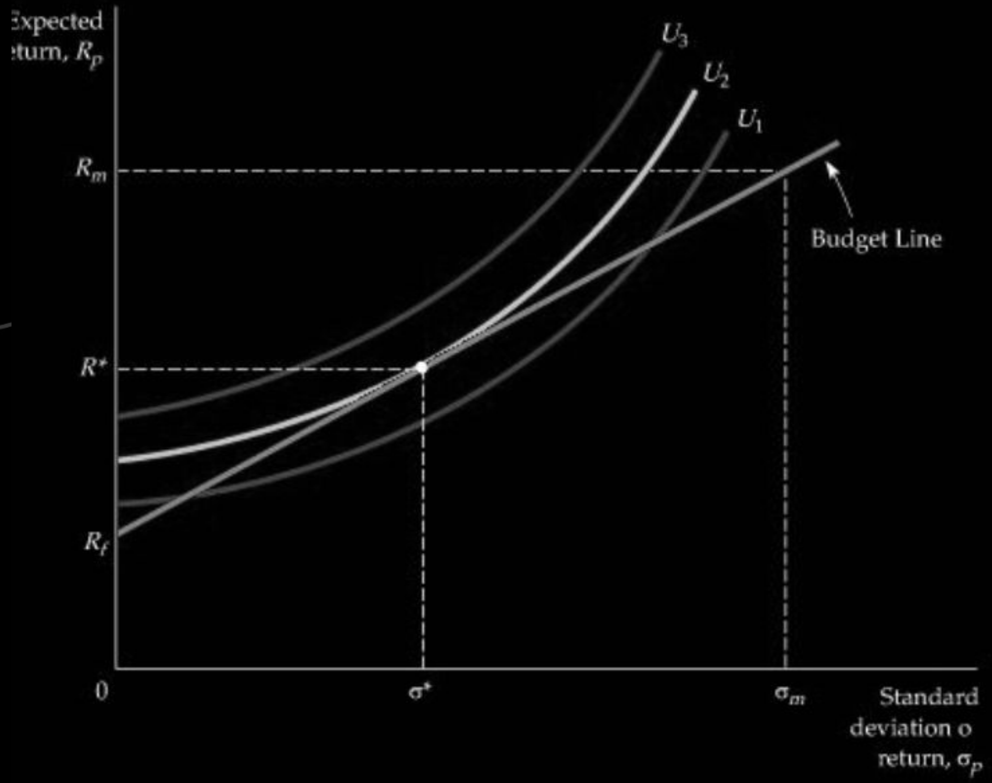
# CAPM & Sharpe Ratio

$$E(R_i) - R_f = \beta_i(R_m - R_f)$$

- Risk premium of a given asset should be the (a) relative volatility of the asset vs the market times (b) the market premium of the asset.
- Takeaway: Higher risk -> higher required return -> more issuance -> more dilution

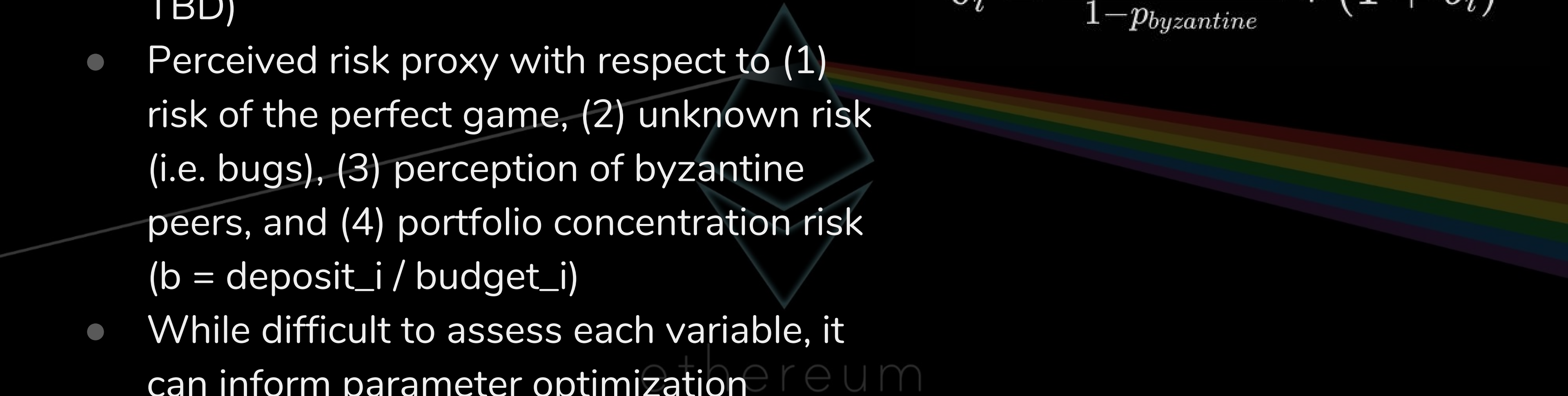
$$S = \left(\frac{R_p - R_f}{\sigma_p}\right)$$

# Risk Return Analysis



Credit: Prentice Hall 2008

# PRR Ratio: Improving the Sharpe Ratio



- “Perceived Risk/Reward” ratio (Name TBD)
- Perceived risk proxy with respect to (1) risk of the perfect game, (2) unknown risk (i.e. bugs), (3) perception of byzantine peers, and (4) portfolio concentration risk (b = deposit_i / budget_i)
- While difficult to assess each variable, it can inform parameter optimization
- More details available on deep-dive post

$$\delta_i = \frac{\sigma_{perfect}+\sigma_{error}}{1-p_{byzantine}} * (1+b_i)$$

# Economic Research Areas

- Participation Constraint Analysis
- Sharpe Ratio and Perceived Risk/Reward Ratio
- Validator Slashing Trilemma 👈🏼 🦄

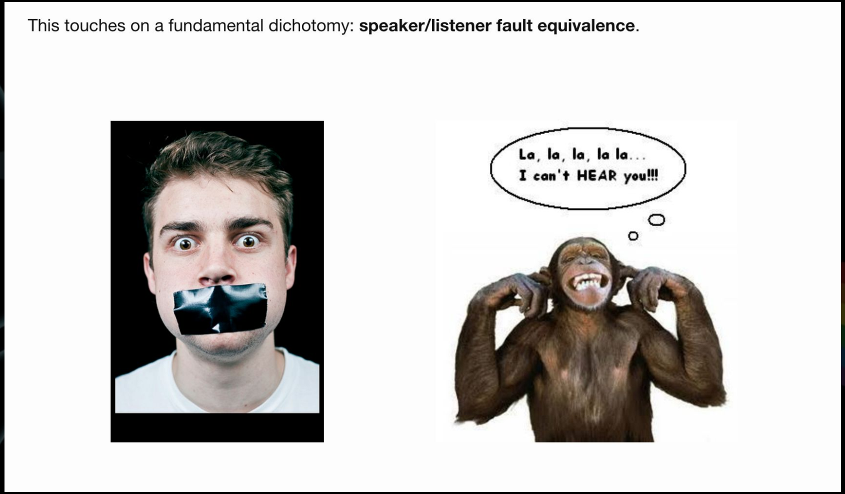
# Validator Slashing Trilemma

# Review: PoW vs PoS

- PoS allows for more design space by allowing validators to retrieve their capital investment.
- However, this requires the protocol to be able to identify and penalize bad actors.
- Slashing conditions (i.e. no double vote, no surround vote) allow for fault attribution, but there is a case in which we cannot perfectly attribute fault.

# Prerequisite: Speaker/Listener Dichotomy

- When we don’t see a vote from  a validator, we can’t tell at the protocol level if the validator was offline or if it wasn’t heard by the rest of the validators.
- When a cartel agree to ignore a set of messages, that is considered a censorship attack

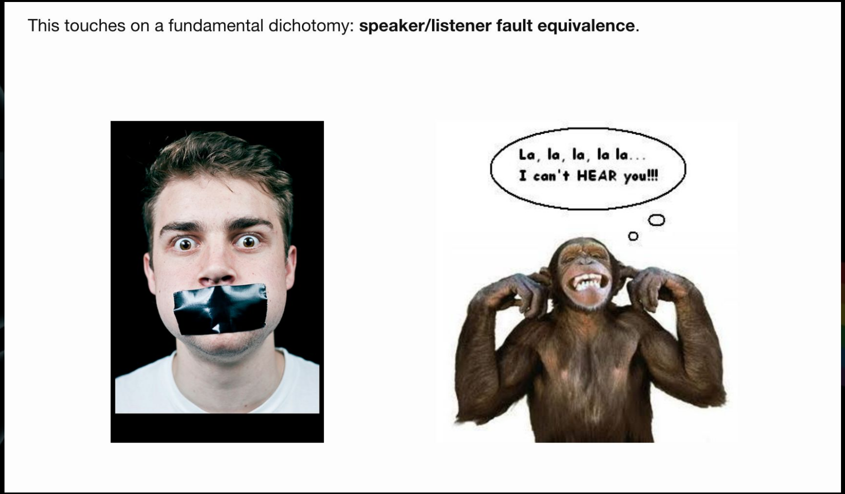


This touches on a fundamental dichotomy: **speaker/listener fault equivalence**.

http://vitalik.ca/general/2017/07/16/triangle_of_harm.html

# Prerequisite: Speaker/Listener Dichotomy

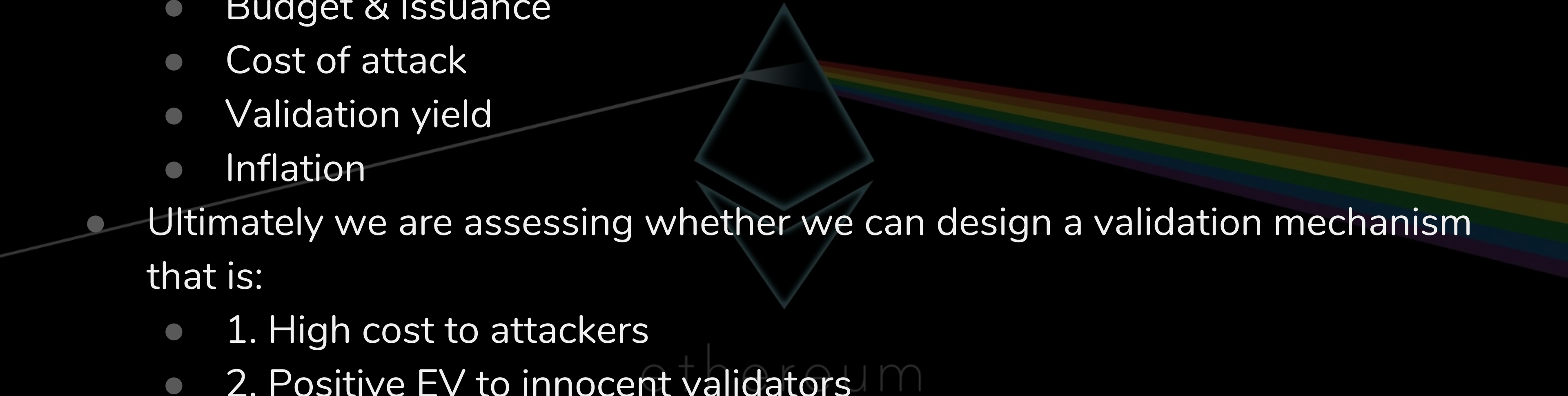
- This requires some level of penalties for both types of validators.
- This externality to honest actors creates a multidimensional optimization problem.



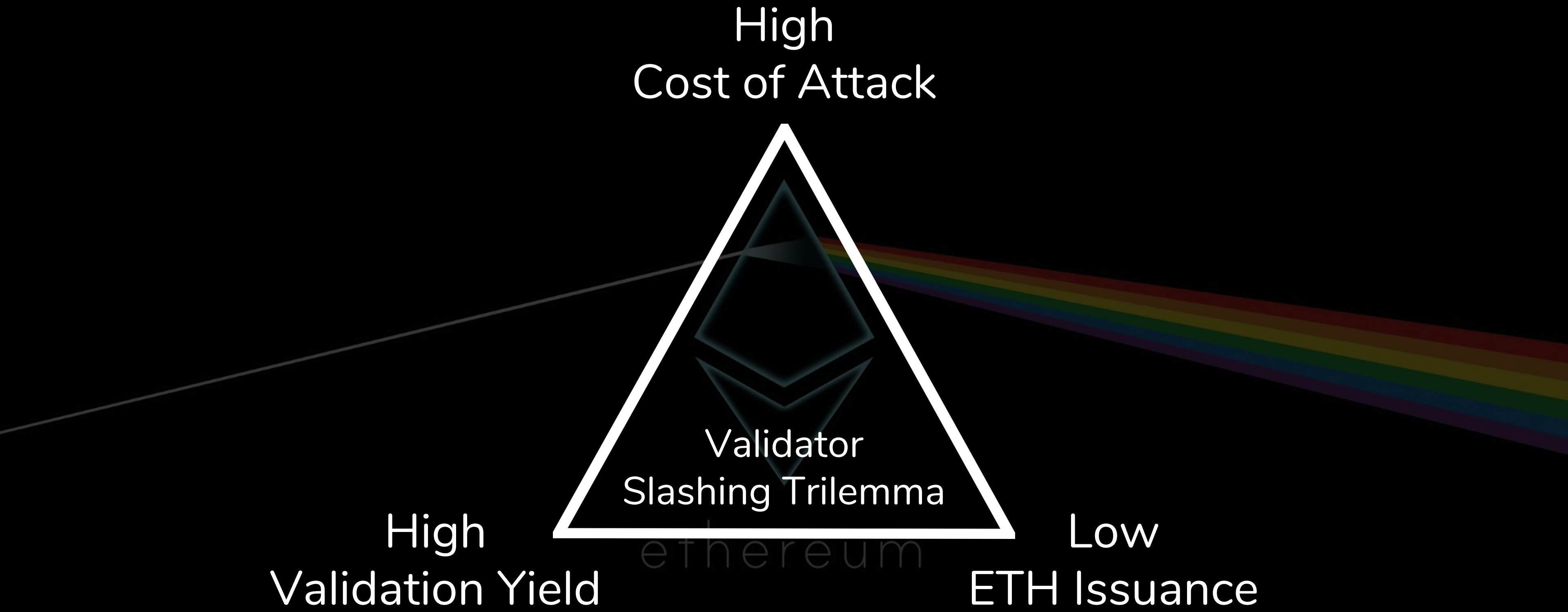
This touches on a fundamental dichotomy: **speaker/listener fault equivalence**.

http://vitalik.ca/general/2017/07/16/triangle_of_harm.html

# Validator Slashing Trilemma



- The research we’ve discussed so far balance:
  - Budget & Issuance
  - Cost of attack
  - Validation yield
  - Inflation
- Ultimately we are assessing whether we can design a validation mechanism that is:
  - 1. High cost to attackers
  - 2. Positive EV to innocent validators
  - 3. Low total rewards

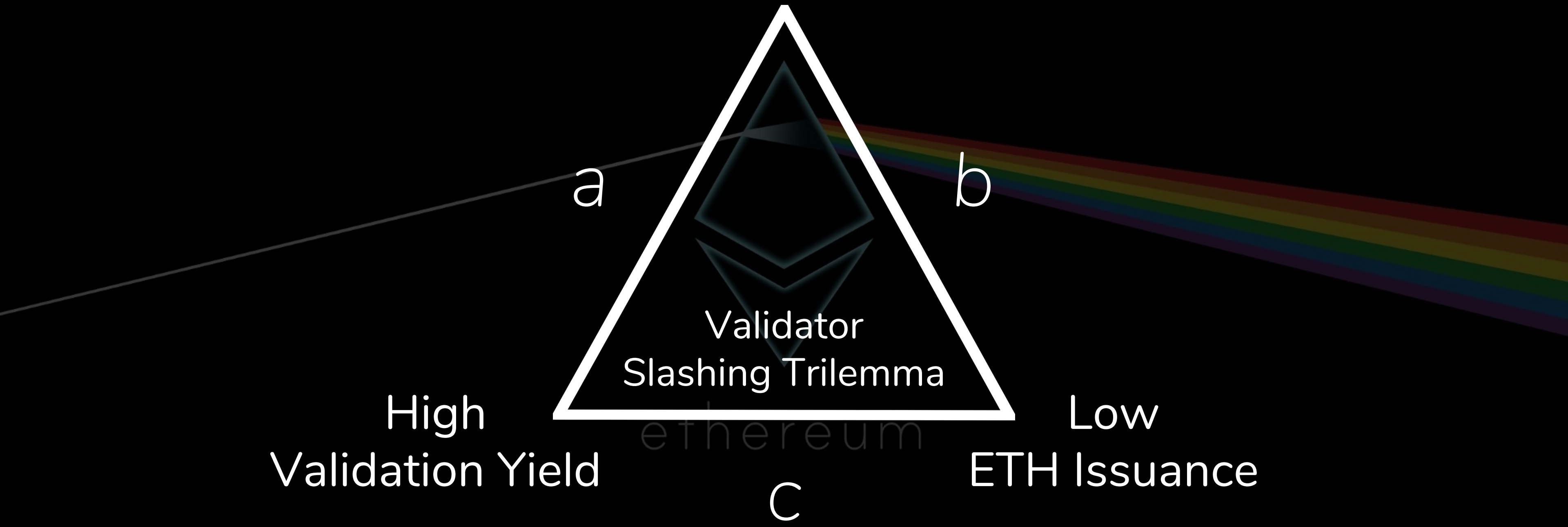


High
Cost of Attack

Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance



High
Cost of Attack

a

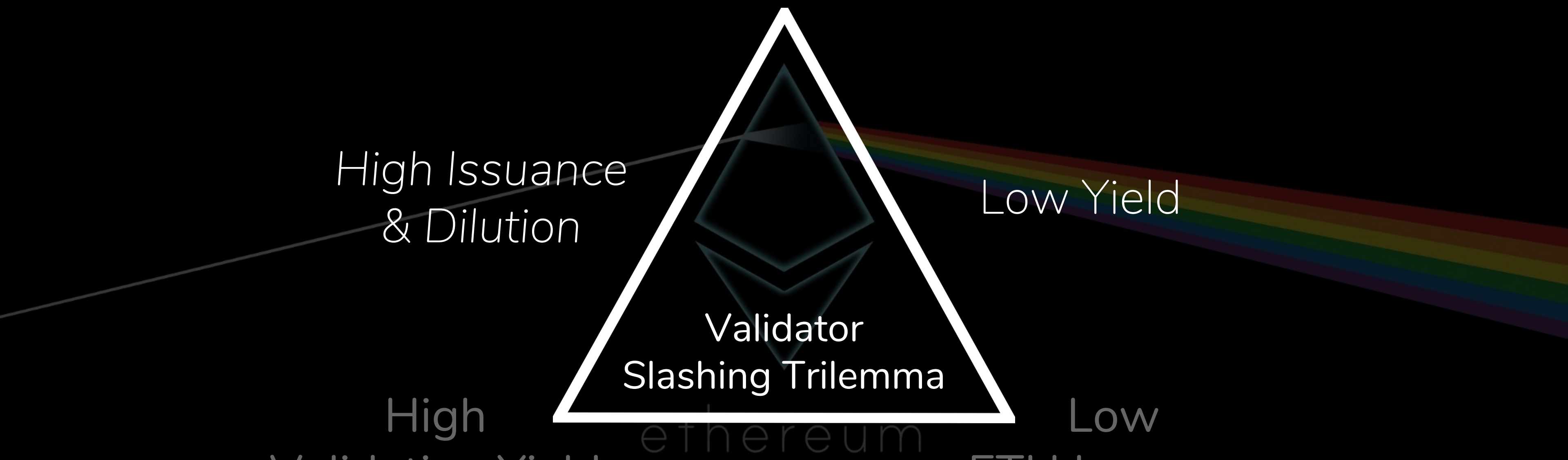
b

Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance

c



High
Cost of Attack

*High Issuance*
*& Dilution*

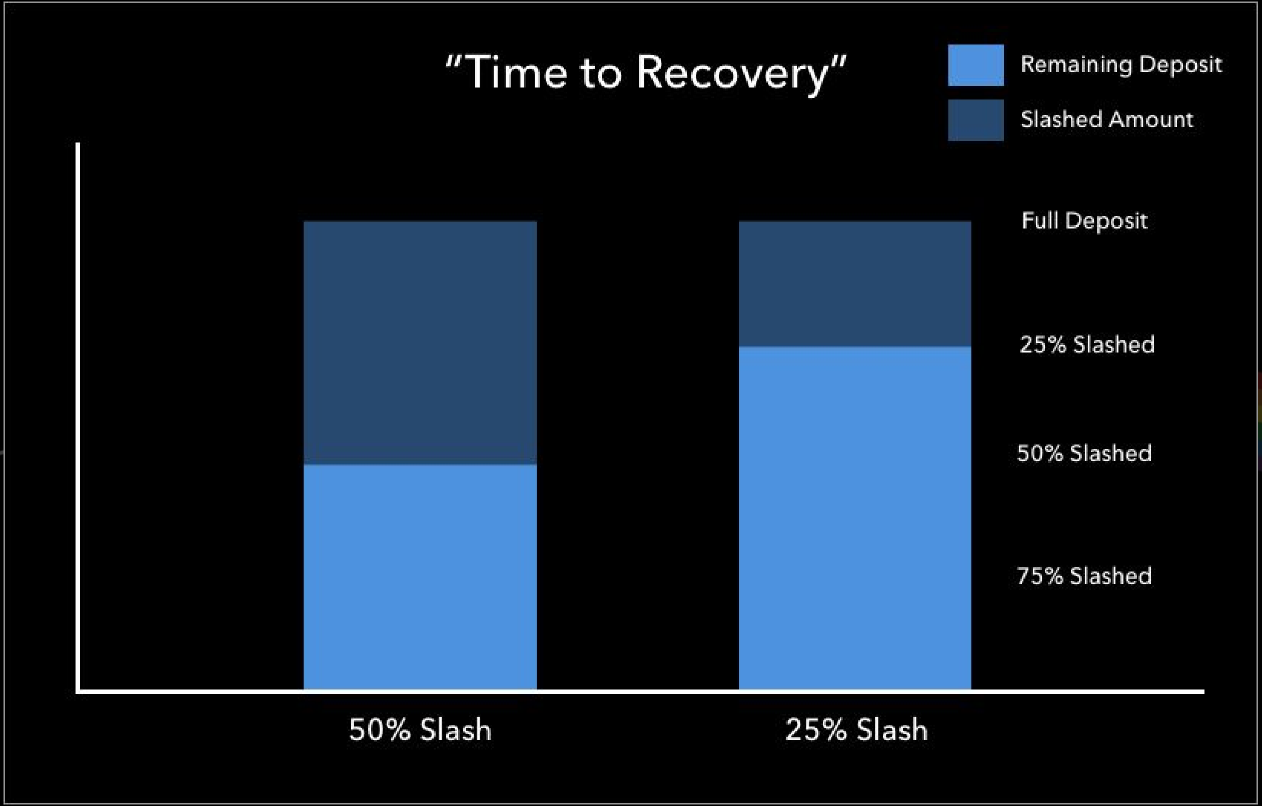
Low Yield

Validator
Slashing Trilemma

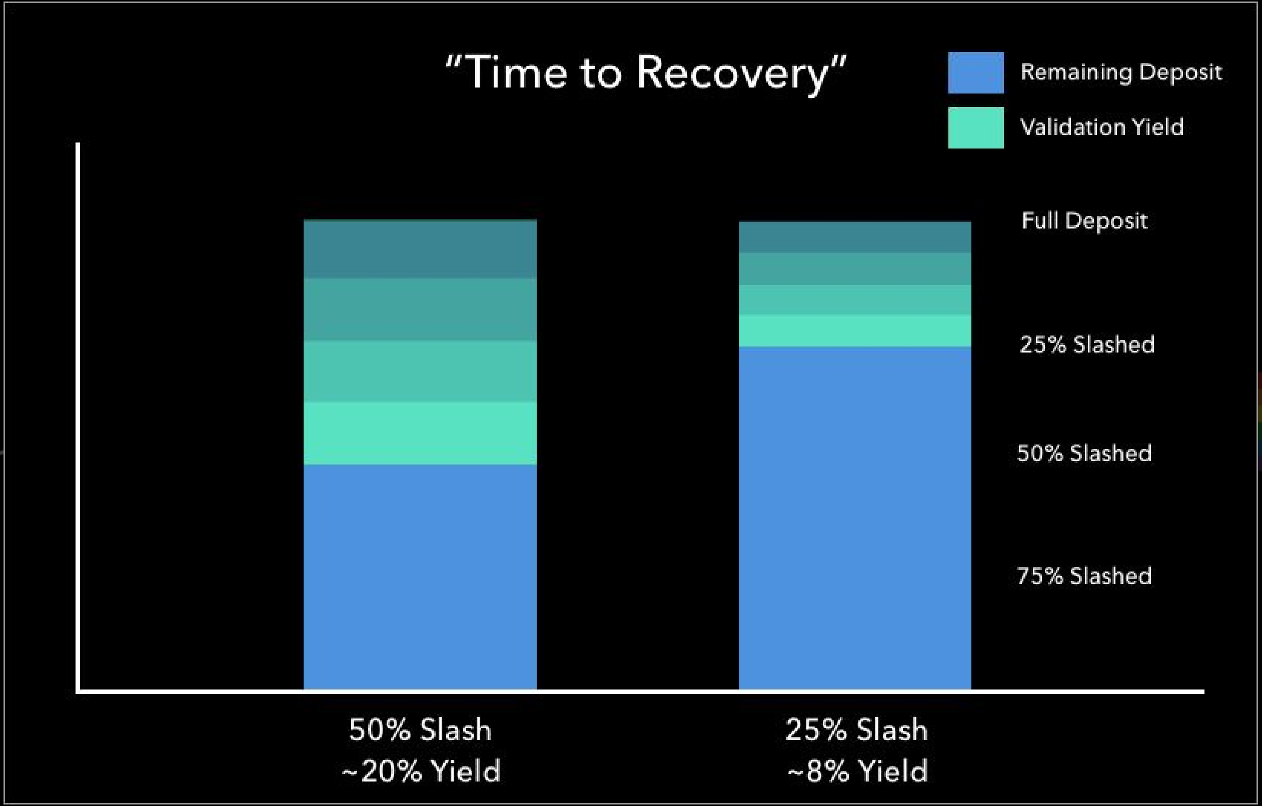
High
Validation Yield

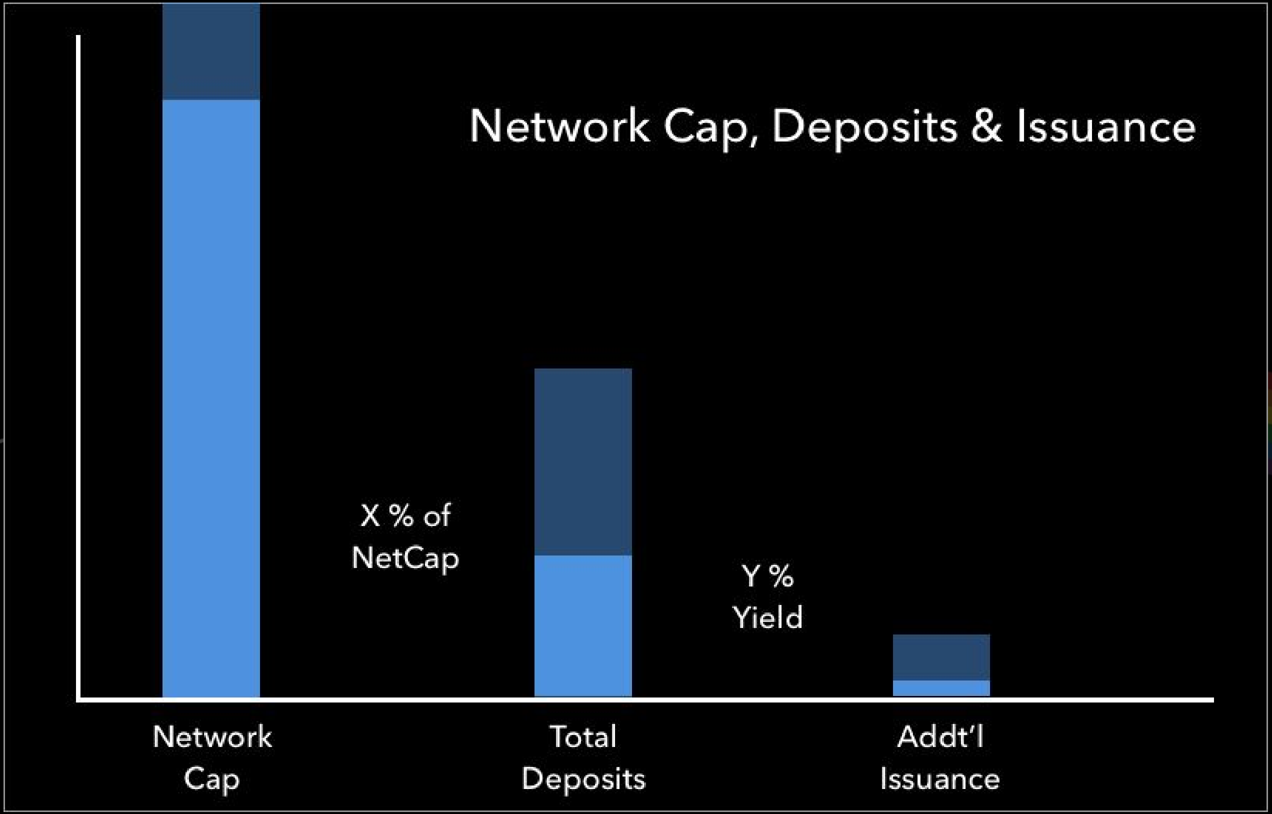
Low
ETH Issuance

Less Draconian
Penalties



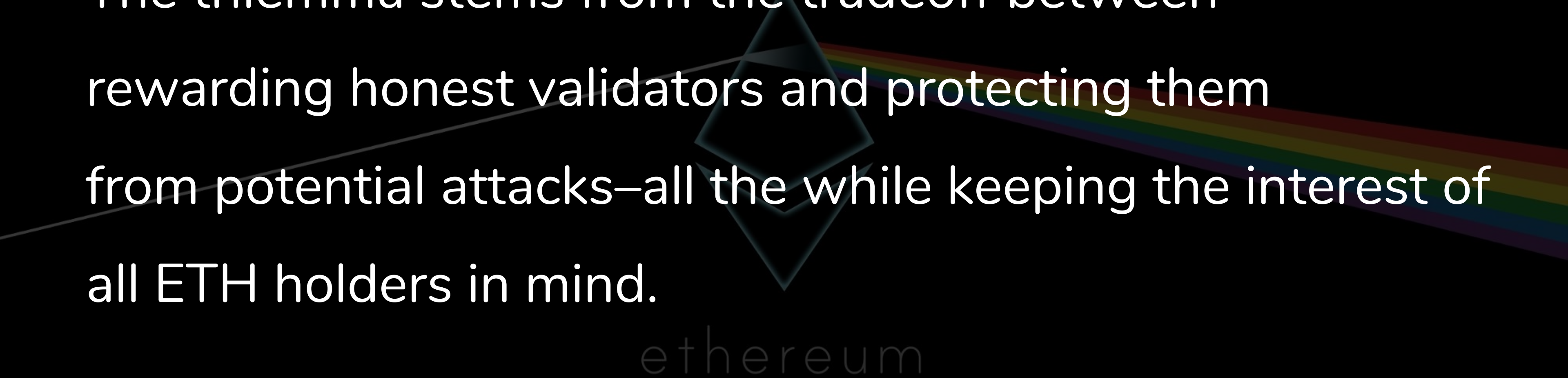
“Time to Recovery”


"Time to Recovery"
Remaining Deposit
Validation Yield
Full Deposit
25% Slashed
50% Slashed
75% Slashed
50% Slash
~20% Yield
25% Slash
~8% Yield



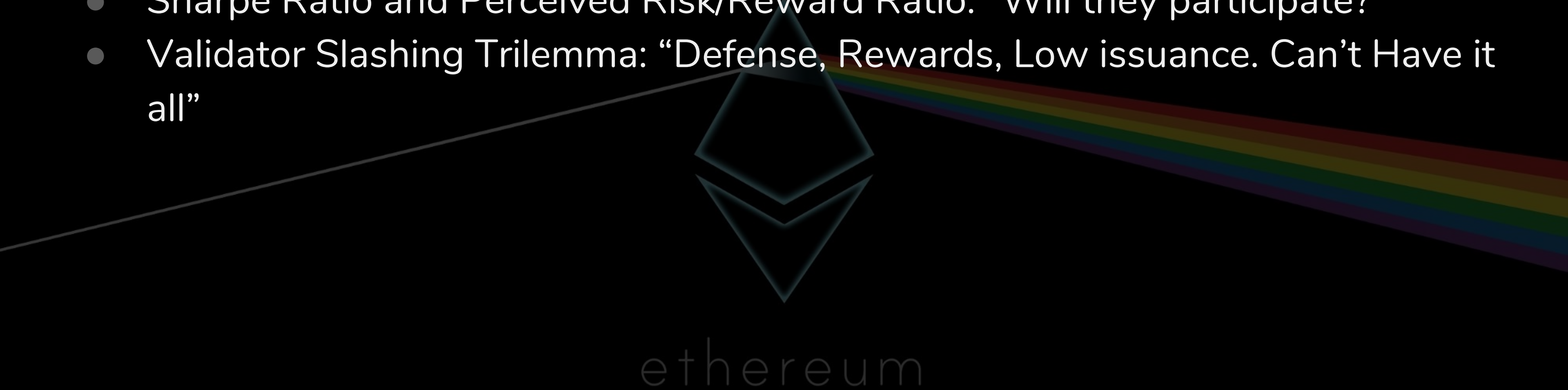
Network Cap, Deposits & Issuance

The trilemma stems from the tradeoff between rewarding honest validators and protecting them from potential attacks–all the while keeping the interest of all ETH holders in mind.



# Economic Research Summary

- Participation Constraint Analysis: “What’s our budget?”
- Sharpe Ratio and Perceived Risk/Reward Ratio: “Will they participate?”
- Validator Slashing Trilemma: “Defense, Rewards, Low issuance. Can’t Have it all”



# Future Work

- Optimizing the parameters
  - Shape of reward/penalties wrt TD, ESF, p_v, result
  - Soft-slashing
  - Withdrawal delay & Deposit vs yield liquidity
  - Ulterior Factor Analysis
- Casper FFG Incentivization Paper
- Optimize parameters in the test network
- Iterate on proposed FFG mechanism design with findings

# To tie it all together...

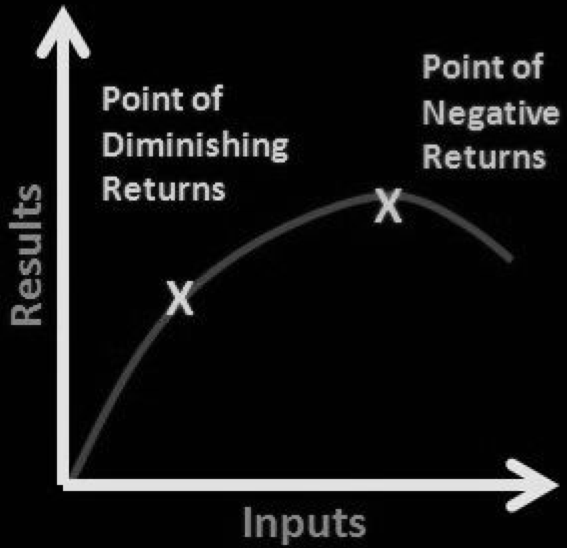
# Conclusion

- We want Casper for energy efficiency, proportional wealth distribution and fine-grained control over incentives (PoS), in addition allows sharding and a gentle transition.
- Cryptoeconomics is the study of the use of incentives to achieve information security objectives.
  - We can incentivize validators to participate with relatively little additional issuance.
  - We have to lower the risk to innocent validators to secure the network economically.
  - There’s a tradeoff among increasing cost of attack, excess returns to validators, and preventing ETH holder dilution.

# Parting thoughts

# Econ Detour: Diminishing Marginal Returns

- Anecdote: real estate value. Trophy assets vs distressed assets.
- Example: Secret Service & the President. The marginal security added by each bodyguard.
    - Ultimately about how much security you need at what cost
- Takeaway: the highest cost of attack is not necessarily the optimal amount of security; the highest yield is not necessarily the most compelling yield. It’s a delicate balance between various things we want.

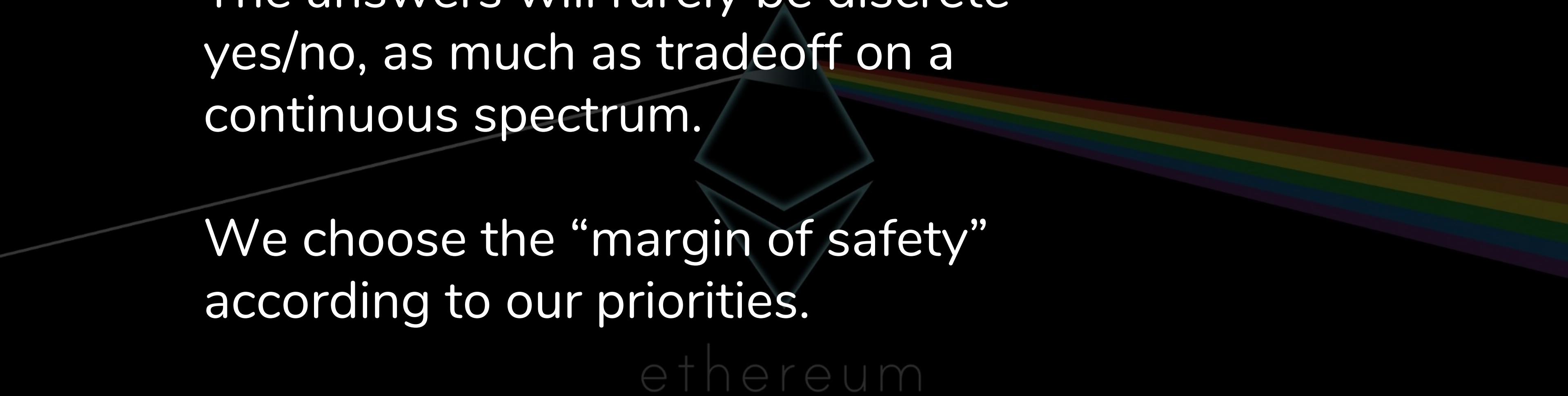


Credit: qph.ec.quoracdn.net

# “Margin of Safety”

- How much buffer do you have from the desired property?
  - Real estate: replacement cost?
- How compelling is the carrot or the stick?
  - I like eating pizza, but at a certain point, I can give up that pizza.
  - I don’t enjoy flying 15 hrs, but at a certain point, I can get on that flight.
- Takeaways: Every behavior has a margin of safety.
- Limitations: large displacements causes deadweight losses

Credit: Seth Klarman



The answers will rarely be discrete yes/no, as much as tradeoff on a continuous spectrum.

We choose the “margin of safety” according to our priorities.

Cryptoeconomics is all about the subtle tradeoffs among desired properties.

There is a price at which great things are OK.

There is a price at which OK things are great.

# Thank you.

questions?
@jon_choi_

# Q&A

- Things I cannot comment on:
  - Timing of roll out
  - Actual constants & parameters
- Things I can comment on:
  - Topics from today
  - Process & approach
- Thank you!

# Appendix

# Liquidity & Value

- "Crypto" Concepts
  - "Slasher" and deposit based PoS
  - Withdrawal Delays
- Economic Concepts
  - Liquidity (LAPM)
  - Opportunity Cost
  - Risk aversion / Loss aversion

# Withdrawal Delay

- Long-range attack and nothing-at-stake
- Liquidity of principal and periodic yield/payments
- LAPM
- Tradeoff between liquidity and longer economic security guarantee (only active bonded payments enable for bonded-PoS security)

# Ulterior Factor Analysis

- ulterior (adj): existing beyond what is obvious or admitted.
- Griefing Factor: “the amount of money lost by the victims divided by the amount of money lost by the attackers”
- Ulterior Factor: “the amount of money gained by attackers outside of the protocol divided by the amount of money lost by the attackers”
  - Price of a directly competing project going up
  - Getting control over the Dapp ecosystem
  - More of the fiat inflows into crypto buying another project instead of ETH.

# Ulterior Factor Analysis

- Cannot directly bound the amount of benefit attackers can have outside of the protocol
- TD/MCap target
  - We want each “attack dollar” to have a lower multiple for affecting the market capitalization of ETH.
- Competitor price correlation.
- As the network’s TD level matures to the ideal levels, griefing factor matters more and ulterior factor matters less

# Priorities of Innocent vs Byzantine

Innocent

1. Capital Preservation
2. Validation Revenue
3. Enthusiasm / Altruism

Byzantine

1. Exoprotocol Gain
2. Loss to Ethereum
3. Capital Preservation