Cryptoeconomics & Casper

Jon Choi

Shenzhen, China

December 3rd, 2017

Objectives

- Explore the definition of “cryptoeconomics” and propose one
- Review why we’re working on Proof of Stake and Casper
- Share the latest cryptoeconomic research

Agenda

- **What is Cryptoeconomics?** **(15min)** 👈🏼 🦄
- **Casper 101** **(10min)**
    - Proof of Stake
    - Casper
- **Cryptoeconomics in Casper** **(15 min)**
    - Participation Constraint
    - CAPM & Sharpe Ratio
    - Liquidity & Opportunity Cost
    - Bayesian Games and Incomplete Information
    - Validator Slashing Trilemma

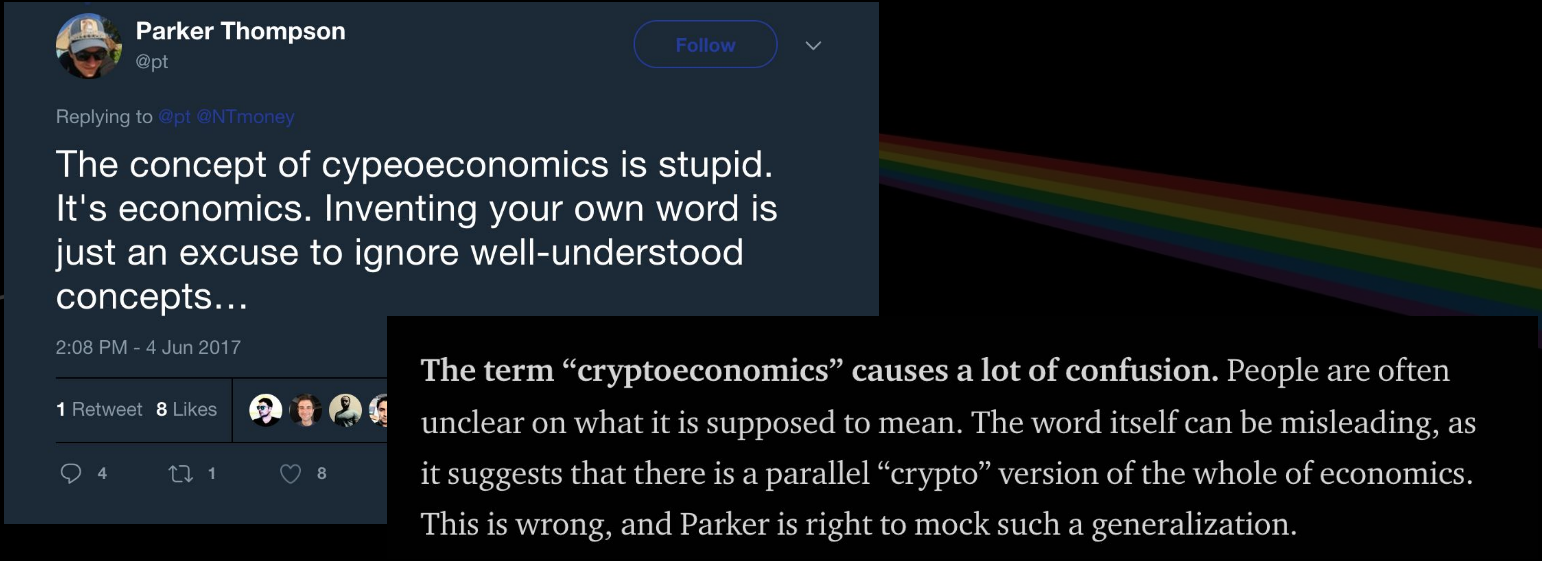
What is Cryptoeconomics?

Cryptoeconomics *noun*

The study of secure transmission of digital scarcity in open networks.

Why bother defining this?

Not universally acknowledged



Parker Thompson
@pt

Replying to @pt @NTmoney

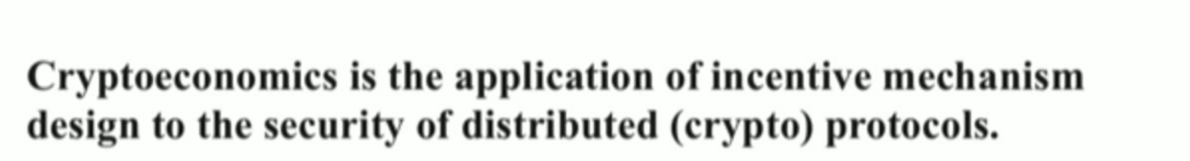
The concept of cypeoeconomics is stupid. It's economics. Inventing your own word is just an excuse to ignore well-understood concepts...

2:08 PM - 4 Jun 2017

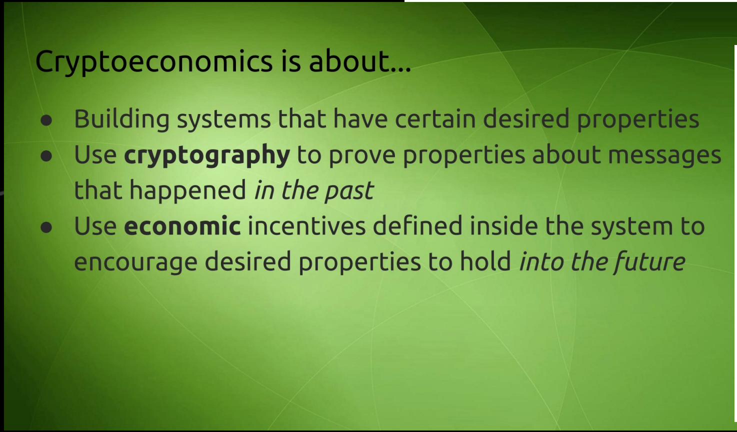
1 Retweet 8 Likes

The term "cryptoeconomics" causes a lot of confusion. People are often unclear on what it is supposed to mean. The word itself can be misleading, as it suggests that there is a parallel "crypto" version of the whole of economics. This is wrong, and Parker is right to mock such a generalization.

No consensus on definition

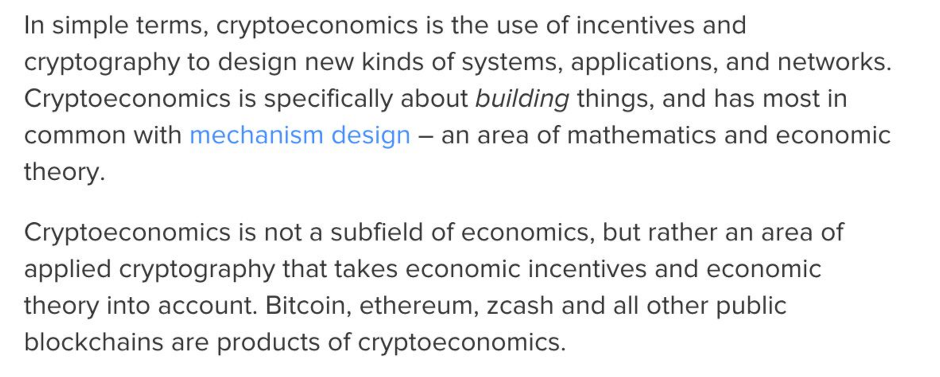


Cryptoeconomics is the application of incentive mechanism design to the security of distributed (crypto) protocols.



Cryptoeconomics is about...

- Building systems that have certain desired properties
- Use **cryptography** to prove properties about messages that happened *in the past*
- Use **economic** incentives defined inside the system to encourage desired properties to hold *into the future*



In simple terms, cryptoeconomics is the use of incentives and cryptography to design new kinds of systems, applications, and networks. Cryptoeconomics is specifically about *building* things, and has most in common with mechanism design – an area of mathematics and economic theory.

Cryptoeconomics is not a subfield of economics, but rather an area of applied cryptography that takes economic incentives and economic theory into account. Bitcoin, ethereum, zcash and all other public blockchains are products of cryptoeconomics.

Building the Definition

Candidate Definitions

- “Design principle that combines cryptography and game theory to create systems that exhibit a set of economic dis/incentives” – ETH Wiki
- “A formal discipline that focuses on the design and characterization of protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy.” – CESC
- “The application of incentive mechanism design to information security problems.” – Vlad Zamfir
- “Use cryptography to prove properties of transactions that happened in the past. Use economic incentives to encourage desired properties to hold in the future.” – VB

Defining a study with other studies

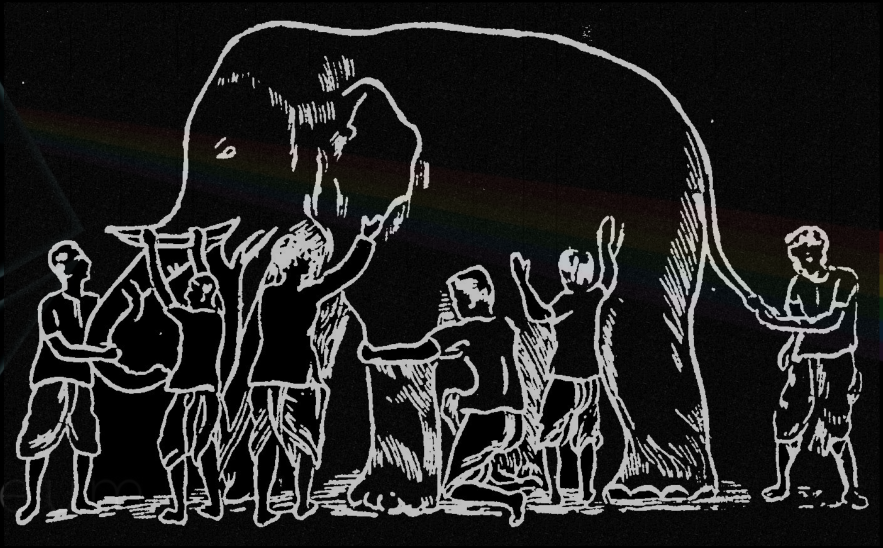
- Because of the multidisciplinary nature of cryptoeconomics, it is natural to define it with other studies.
  - “Economics of blockchains,” “Incentives in decentralized systems,” “Applying game theory & mechanism design to applied cryptography / decentralized networks”
- While those derived definitions are very accurate and thorough, it doesn’t provide an intuitive guide to newcomers because it abstracts away [the fundamental concepts which may seem complex]
- Also, it often creates tension around what CE is a subfield of.
- So let’s define CE without using the words “blockchain,” “economics,” “game theory,” “mechanism design,” “cryptography,” “cryptocurrency,” “decentralized,” etc.

The Objective

- We can learn from the definition of other studies
  - Mathematics – “the abstract science of number, quantity, and space.”
  - Psychology – “the scientific study of the human mind and its functions.”
  - Philosophy – “the study of the fundamental nature of knowledge, reality, and existence.”

The properties of cryptoeconomics

- Open network of computers that communicate with each other
- Mathematical proofs that hide information in open communication channels
- Maximizing profit against the competition
- Aligning the interest of the individual with the interest of the entire ecosystem

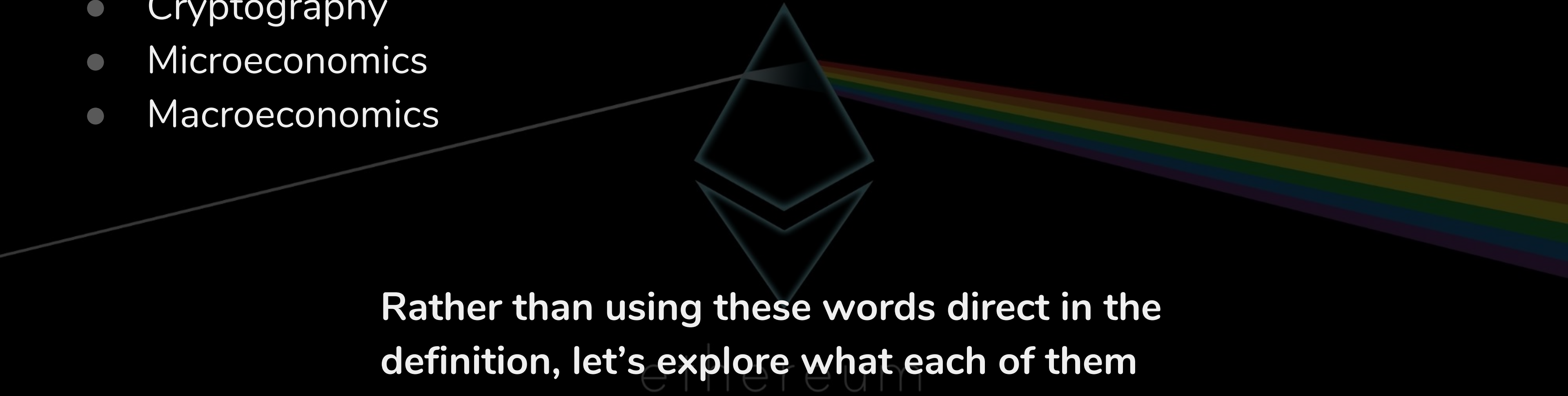


The ingredients

- Distributed Systems
- Cryptography
- Microeconomics
- Macroeconomics

The ingredients

- Distributed Systems
- Cryptography
- Microeconomics
- Macroeconomics

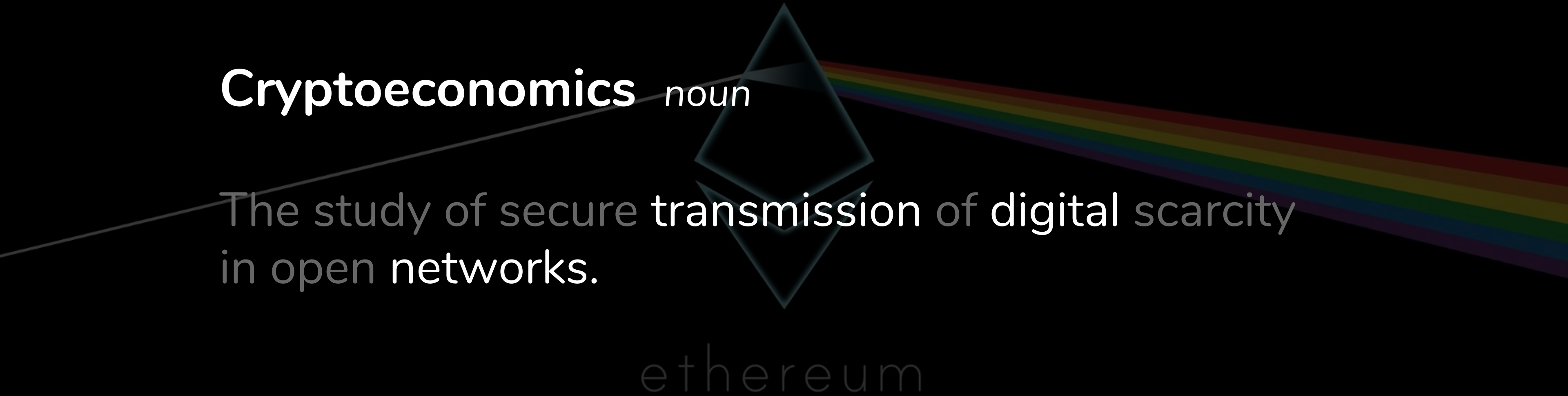


Rather than using these words direct in the definition, let’s explore what each of them study to synthesize a definition.

Distributed Systems

- “A collection of autonomous, programmable, asynchronous and failure-prone entities that communicate through an unreliable communication medium”
    - Telecommunications
        - Internet, cellular
    - Network applications
        - WWW, bitorrent, MMORPGs
    - Cloud computing
    - Cryptocurrencies
- Study of communication networks

Distributed Systems



Cryptoeconomics *noun*

The study of secure transmission of digital scarcity in open networks.

Cryptography

- "Secure communication in the presence of third party adversaries"
  - Public Key Cryptography
    - Tool for asymmetry
  - Allows for open networks
  - Defends against adversaries in the network
- Study of privacy in open contexts

Cryptography

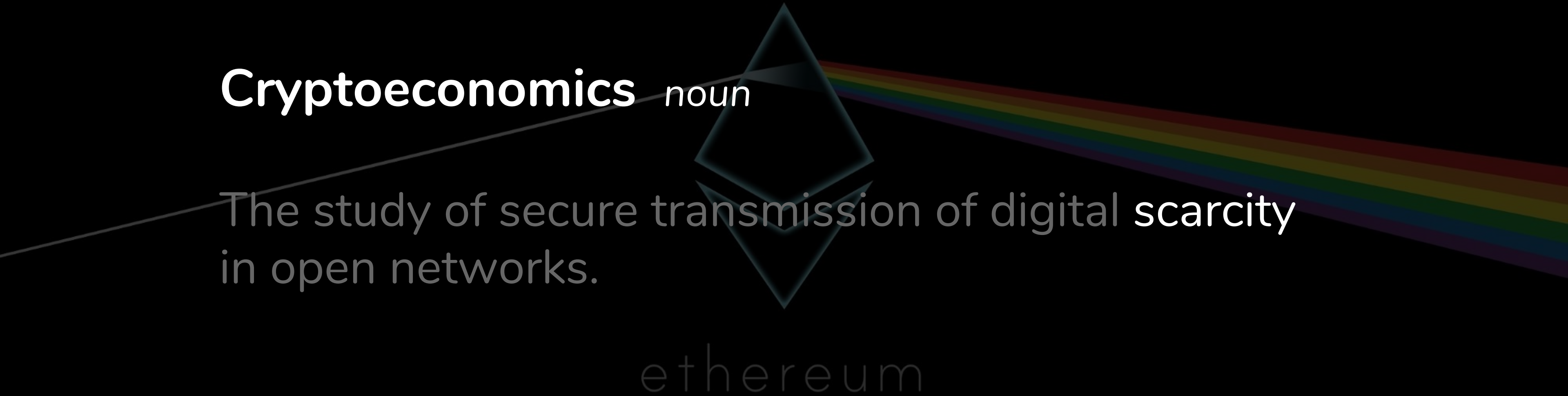
Cryptoeconomics *noun*

The study of secure transmission of digital scarcity in open networks.

Microeconomics

- “the part of economics concerned with single factors and the effects of individual decisions.”
  - Opportunity Cost
  - Cost of Capital
  - Time Value of Money
  - Economies of Scale
  - Competition (Oligopolies)
  - Game Theory
  - Mechanism Design
- The study of scarcity

Microeconomics



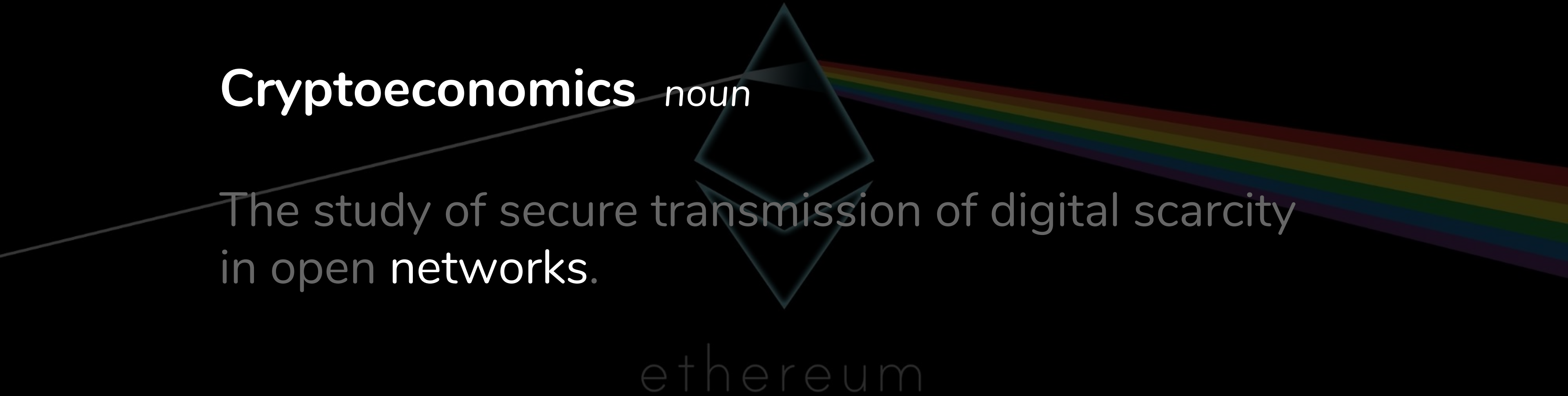
Cryptoeconomics *noun*

The study of secure transmission of digital scarcity in open networks.

Macroeconomics

- “the part of economics concerned with large-scale or general economic factors, such as interest rates and national productivity.”
    - Inflation
    - Wealth distribution
    - Economy of economies
        - Network of smaller economies
- Study of economic ecosystems

Macroeconomics



Cryptoeconomics *noun*

The study of secure transmission of digital scarcity in open networks.

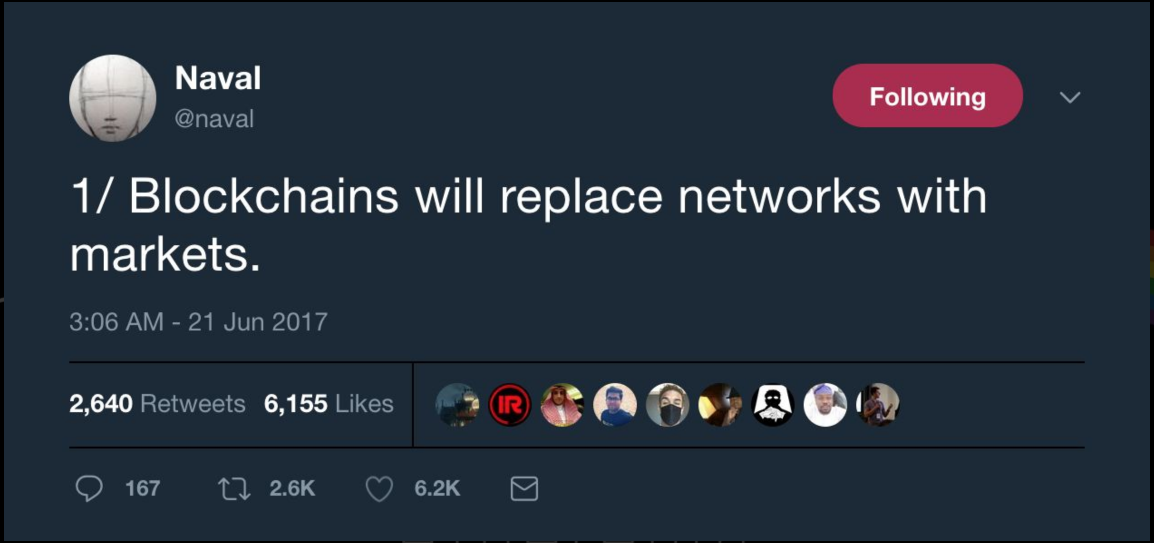
A breakthrough in any of the components can differentiate a winning cryptoeconomic model, and a vulnerability in any of the components can also compromise an otherwise successful cryptoeconomic model.

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

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.

Why does it matter?

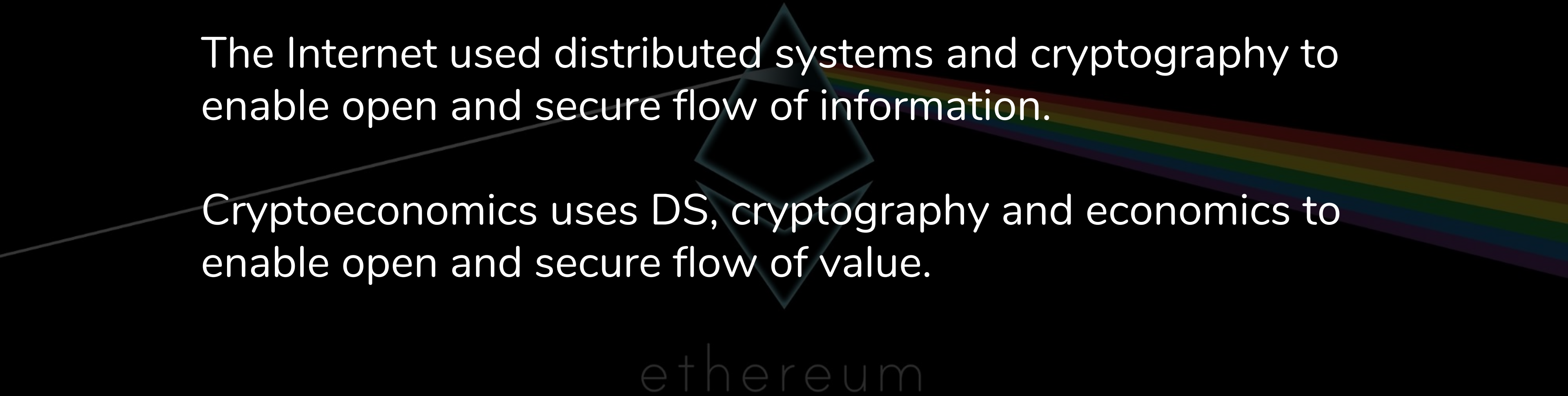


Naval
@naval

1/ Blockchains will replace networks with markets.

3:06 AM - 21 Jun 2017

2,640 Retweets 6,155 Likes



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.

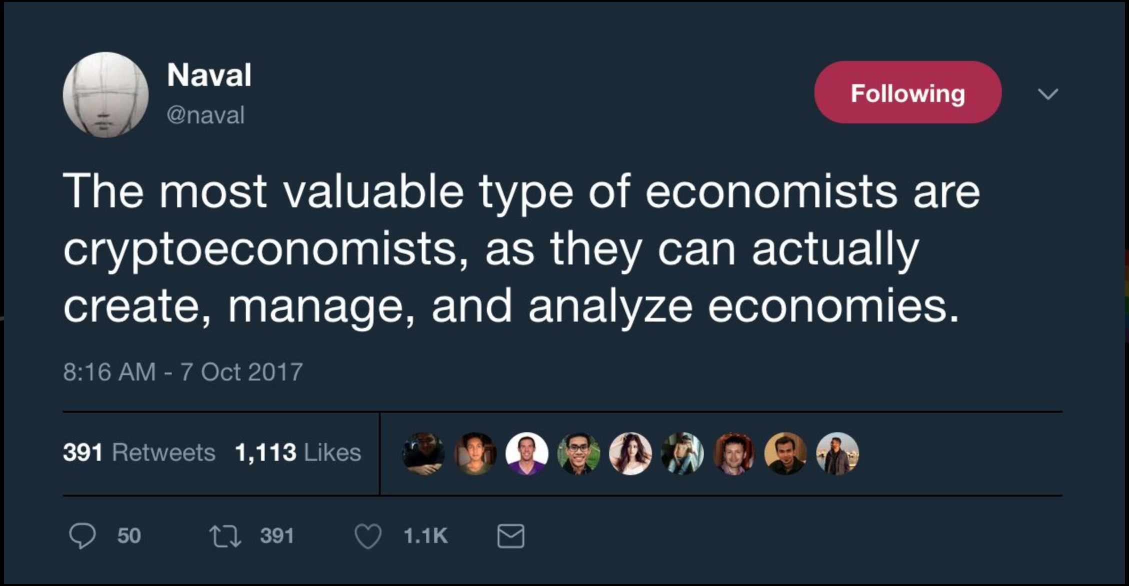
The Internet enabled Google, Facebook, Amazon, Apple to connect the world–under their third-party custody.

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.

“You cannot reason about a security of blockchain consensus protocols without reasoning about economics.”

– Vitalik Buterin



Naval
@naval

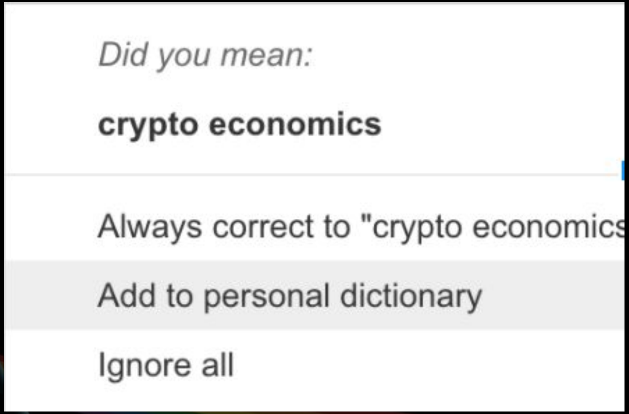
The most valuable type of economists are cryptoeconomists, as they can actually create, manage, and analyze economies.

8:16 AM - 7 Oct 2017

391 Retweets 1,113 Likes

Cryptoeconomics *noun*

The study of secure transmission of digital scarcity in open networks.


Did you mean:
crypto economics
Always correct to "crypto economics
Add to personal dictionary
Ignore all

Cryptoeconomics *noun*

The study of secure transmission of digital scarcity in open networks.

Agenda

- **What is Cryptoeconomics?** **(15min)**
- **Casper 101** **(10min)**
  - Proof of Stake 👈🏼 🦄
  - Casper
- **Cryptoeconomics in Casper** **(15 min)**
  - Participation Constraint
  - CAPM & Sharpe Ratio
  - Liquidity & Opportunity Cost
  - Bayesian Games and Incomplete Information
  - Validator Slashing Trilemma

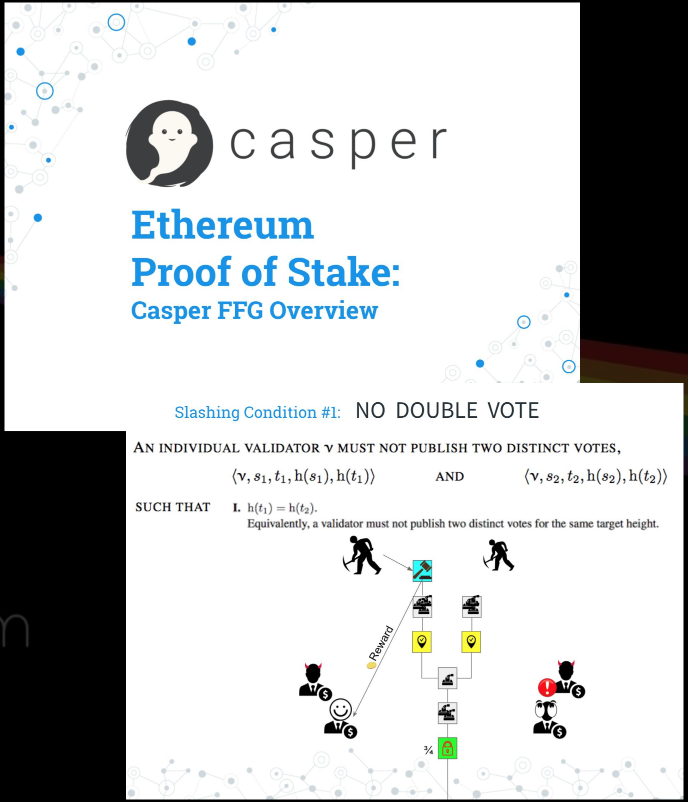
Casper implements proof of stake in Ethereum

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.

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

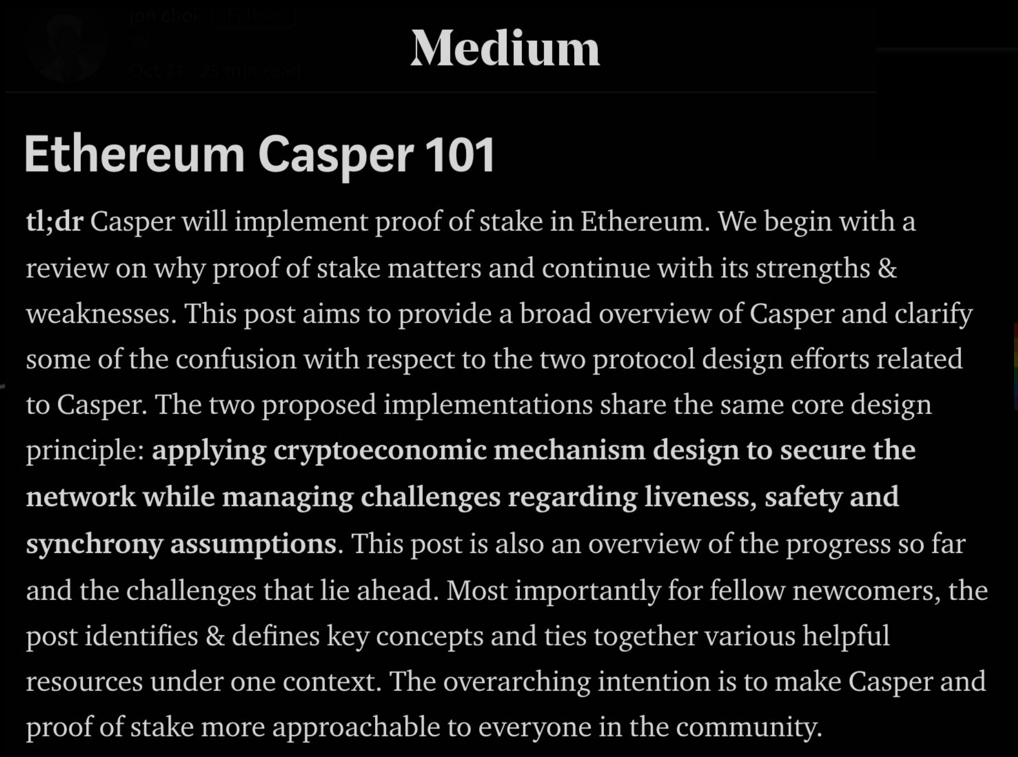
Slashing Condition #1: NO DOUBLE VOTE

AN INDIVIDUAL VALIDATOR ν 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.

Medium



jon choi

Oct 21 · 25 min read

Ethereum Casper 101

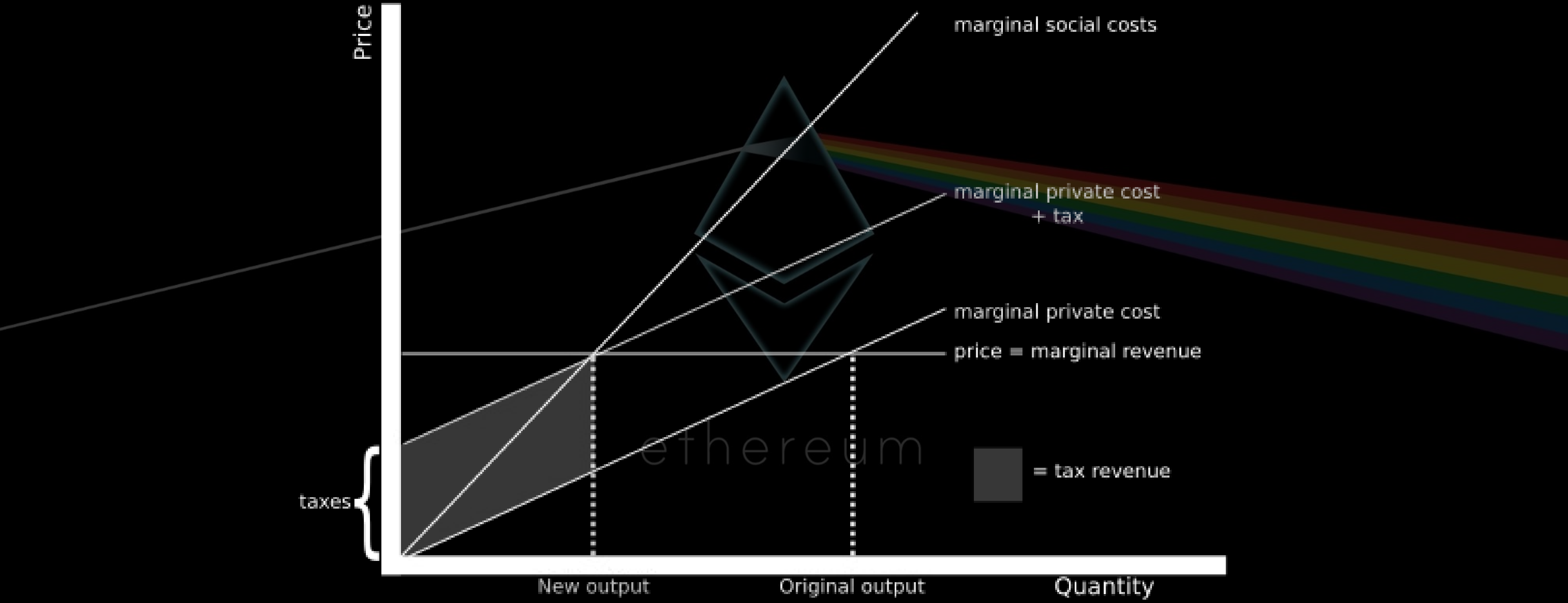
tl;dr Casper will implement proof of stake in Ethereum. We begin with a review on why proof of stake matters and continue with its strengths & weaknesses. This post aims to provide a broad overview of Casper and clarify some of the confusion with respect to the two protocol design efforts related to 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

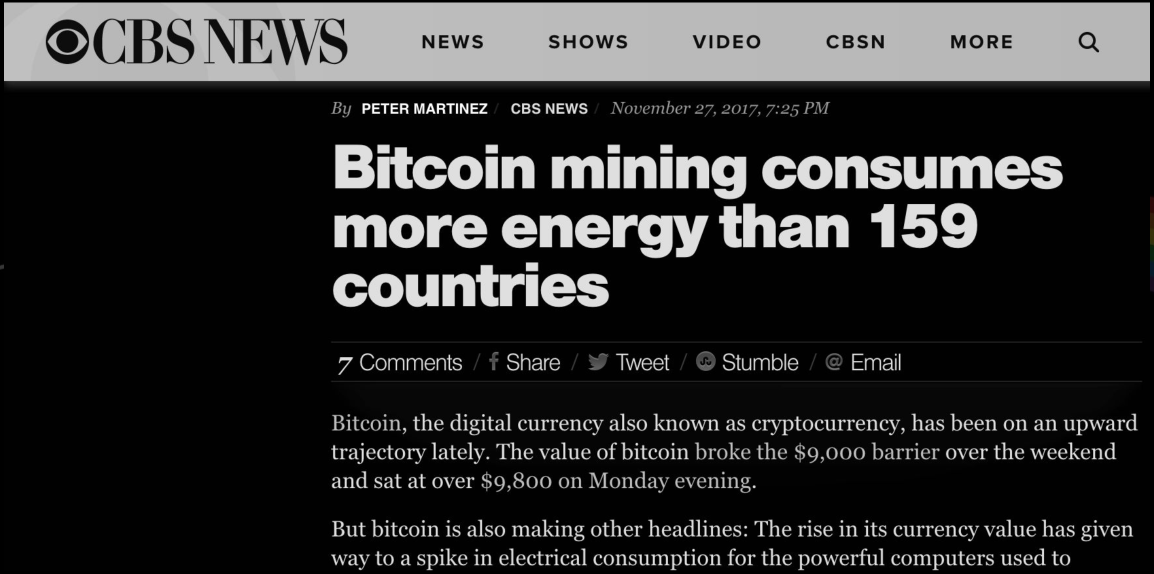
1. Energy Efficiency

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

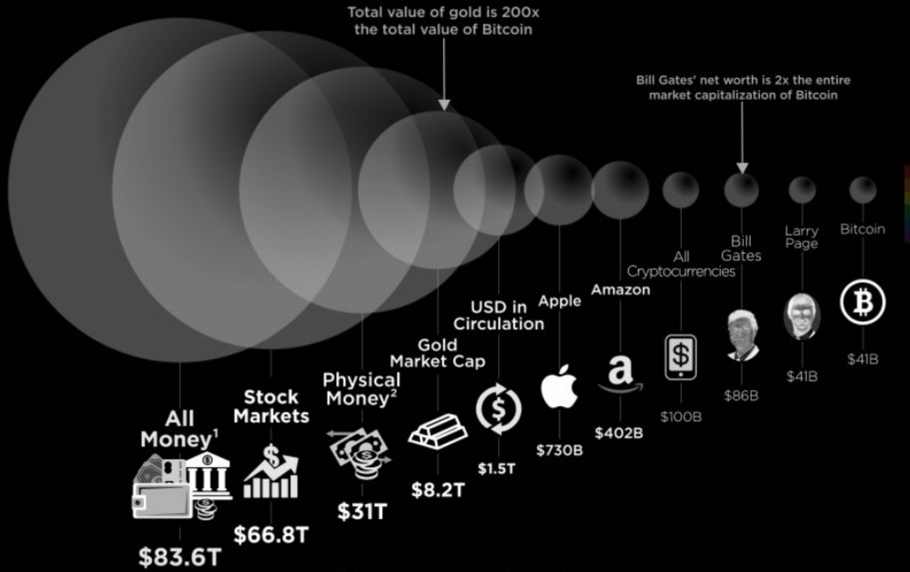
Bitcoin, the digital currency also known as cryptocurrency, has been on an upward trajectory lately. The value of bitcoin broke the $9,000 barrier over the weekend and sat at over $9,800 on Monday evening.

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.

Putting the World’s Money into Perspective



Total value of gold is 200x the total value of Bitcoin

Bill Gates’ net worth is 2x the entire market capitalization of Bitcoin

Sources:
https://howmuch.net/articles/worlds-money-in-perspective
https://coinmarketcap.com
https://www.forbes.com
https://www.federalreserve.gov
https://www.cia.gov

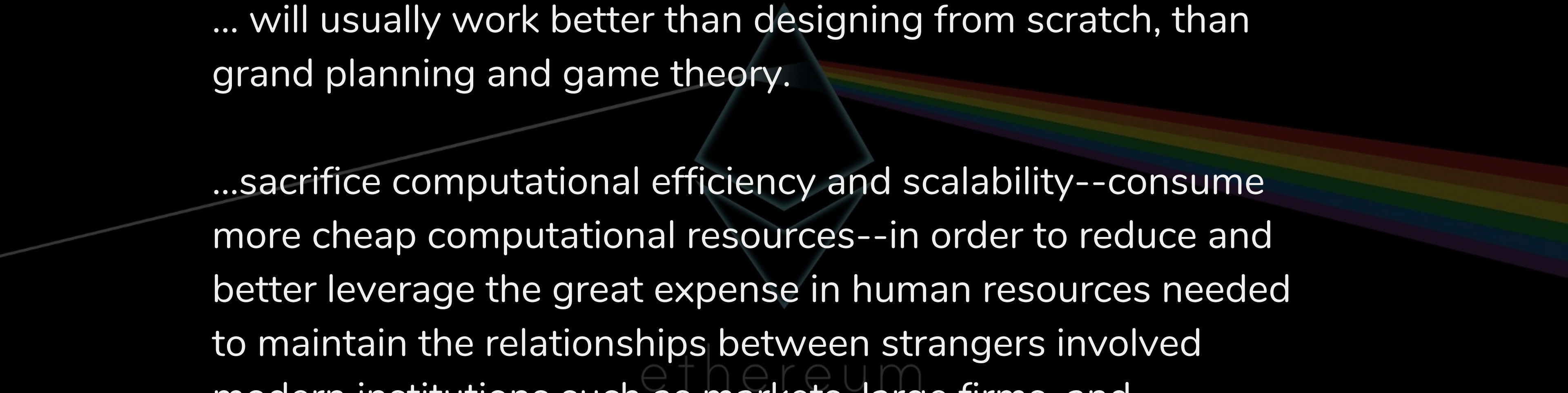
[1] All Money = money in any form including bank or other deposits as well as notes and coins.

[2] Phisical Money = money in forms that can be used as a medium of exchange, generally notes, coins, and certain balances held by banks.

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

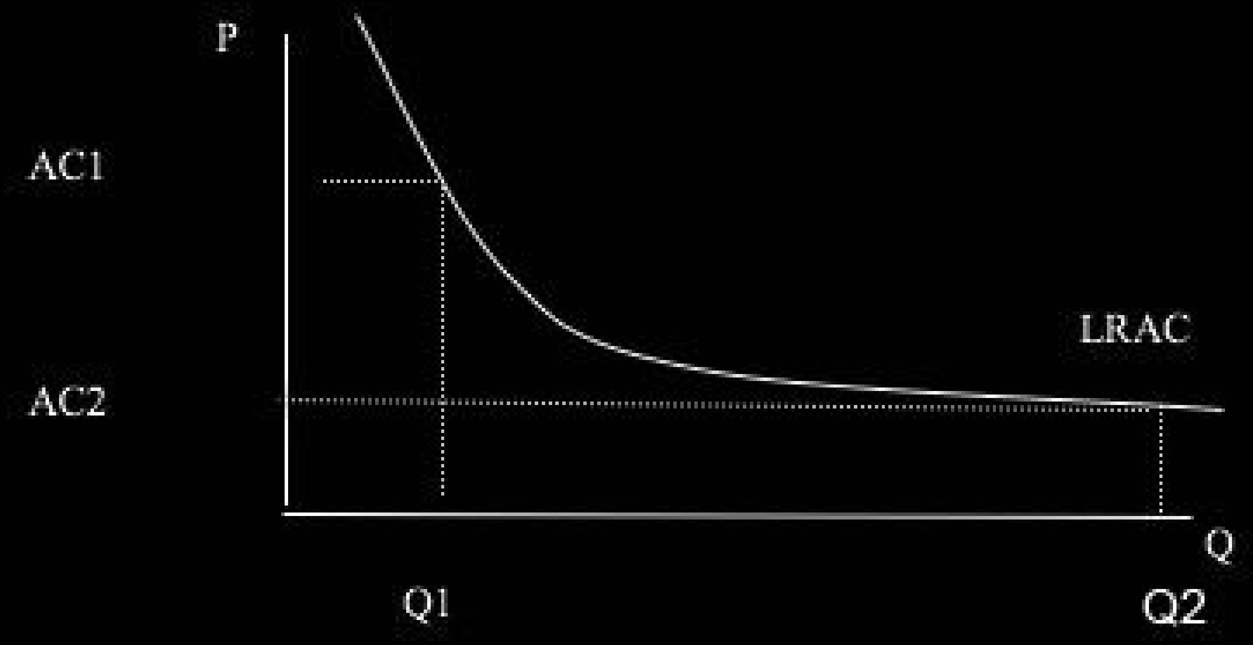
- Example: Public Transit Ticketing
  - Realized cost: Have everyone take 2 minutes to load their transit card and pay per trip.
  - Risk of Loss: Honor system, but if you’re caught without a ticket, you get a fine that’s worth a 100 trips.
- Social Scaling: better global outcome to pool taxes and create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

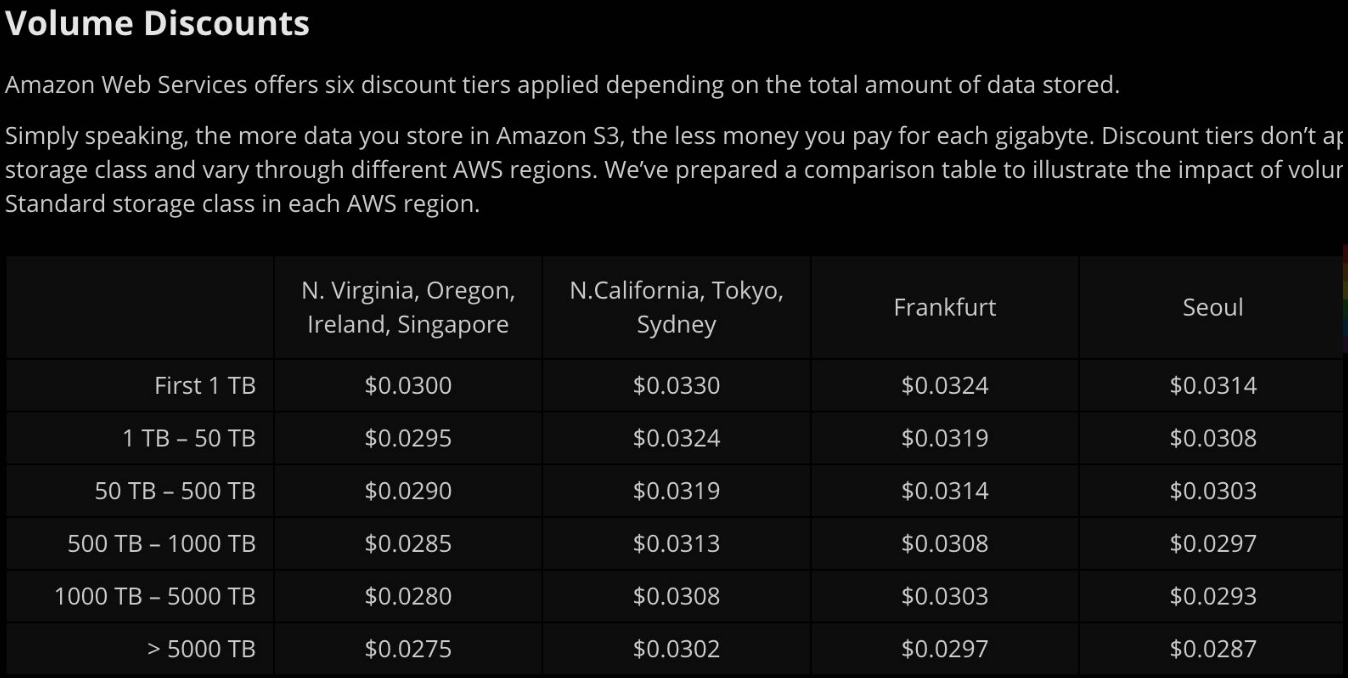


Credit: economicshelp.org

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.

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.

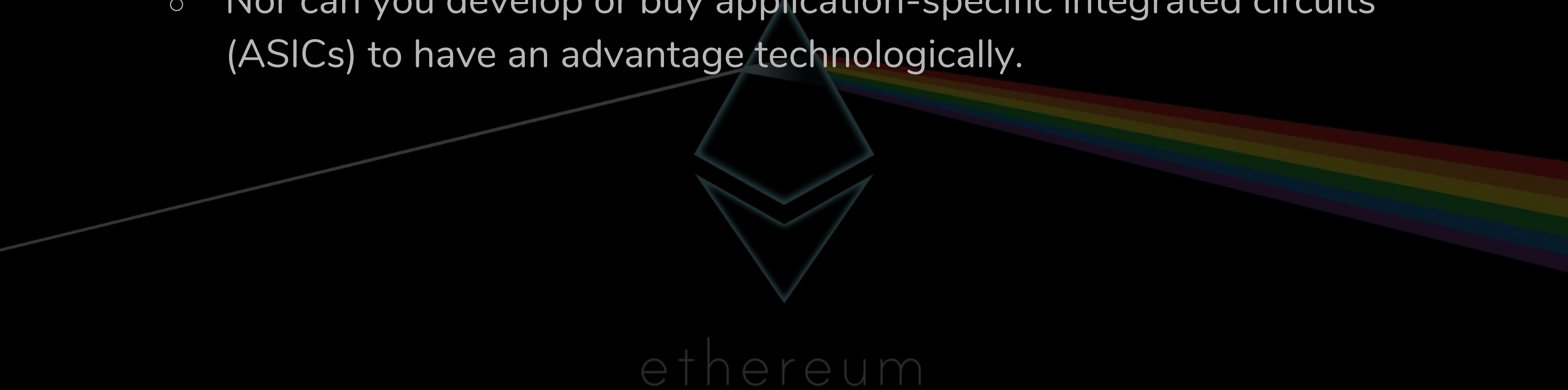
	N. Virginia, Oregon, Ireland, Singapore	N.California, Tokyo, Sydney	Frankfurt	Seoul
First 1 TB	$0.0300	$0.0330	$0.0324	$0.0314
1 TB – 50 TB	$0.0295	$0.0324	$0.0319	$0.0308
50 TB – 500 TB	$0.0290	$0.0319	$0.0314	$0.0303
500 TB – 1000 TB	$0.0285	$0.0313	$0.0308	$0.0297
1000 TB – 5000 TB	$0.0280	$0.0308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

Credit: AWS

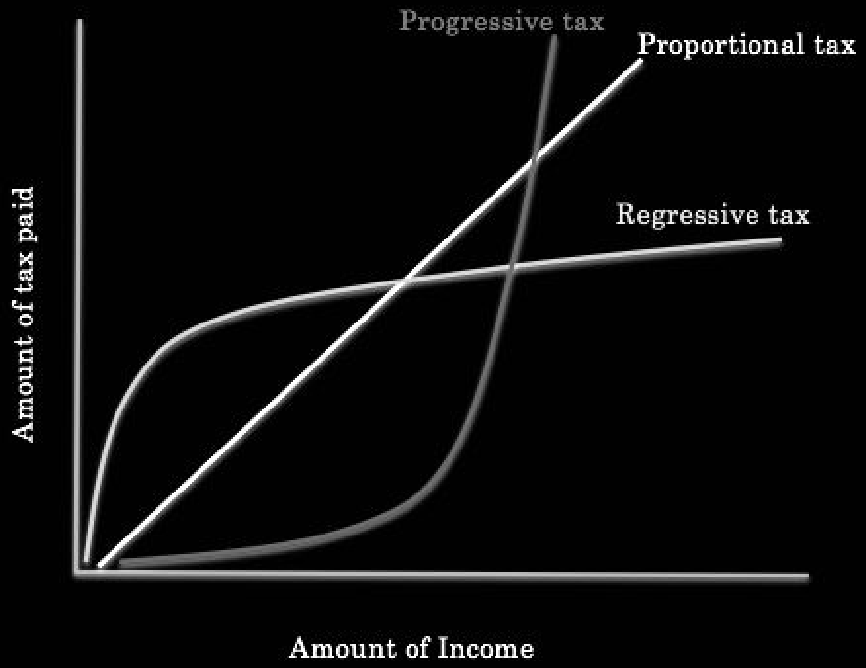
This means that two sets of mining pools with equal economic cost, one may be able to achieve a higher hash rate and have more influence in the network, dollar for dollar.

“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. Explicit Economic Security

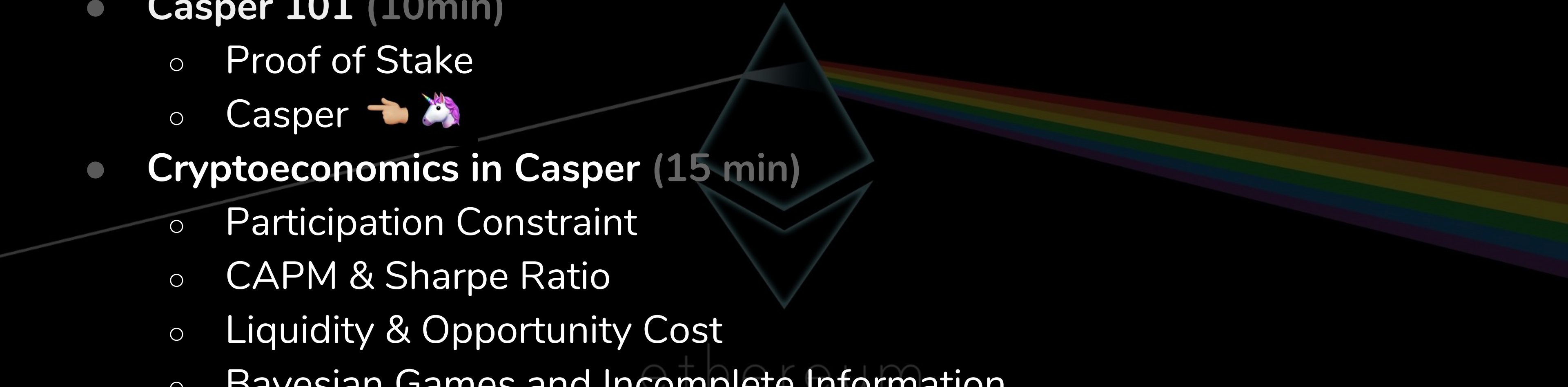
Explicit Economic Security

- In PoW, your downside is capped at how much energy cost and hardware depreciation you incur and therefore has an implicit cost that adjusts dynamically (via 10 min block time target).
- PoS has the flexibility to explicitly design the penalties of Byzantine behavior.
    - This gives the protocol designer increased control over dialing in the “shape” of the asymmetric risk & reward profile of various actions within the network.
- One proxy for security is the cost of doing damage to the utility and correctness of the network, and therefore the ability to have explicit penalties (perhaps at levels that are more draconian than PoW) can increase the security of the network (i.e. economic security).
    - “the cost profile of a repeated 51% attack in PoS is as if “your ASIC farm burned down” with each additional round.”

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.

Agenda



- **What is Cryptoeconomics?** **(15min)**
- **Casper 101** **(10min)**
    - Proof of Stake
    - Casper 👈🏼 🦄
- **Cryptoeconomics in Casper** **(15 min)**
    - Participation Constraint
    - CAPM & Sharpe Ratio
    - Liquidity & Opportunity Cost
    - Bayesian Games and Incomplete Information
    - Validator Slashing Trilemma

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

Finality & Scaling

Casper & Scaling

- Casper is about establishing explicit finality (as opposed to probabilistic finality)
- Explicit finality enables maintaining network security while scaling via sharding.

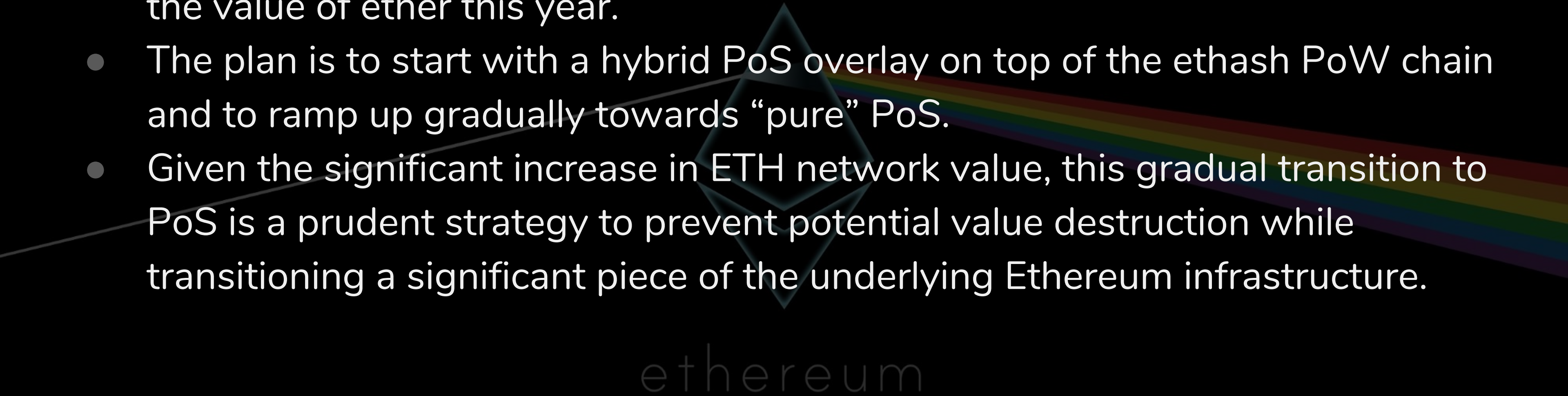
Finality not for simple txs but for scaling

- So to go back to the point, if we are to explore each node in the network “doing less” or “knowing less,” it is hugely beneficial to consider only the past few epochs of finality rather than the entire probabilistic chain since the genesis block.
- Therefore, at this epoch time interval, finality doesn’t actually help with confirming a simple transaction, since transactions clear in number of confirmations fewer than the epoch time.
- Instead, finality will enable public blockchains to scale beyond the current ~10 transactions per second to larger orders of magnitude.

Stepping Stone to Pure PoS

Gentle Transition

- Ethereum’s explicit goals to move to PoS predates the significant increase in the value of ether this year.
- The plan is to start with a hybrid PoS overlay on top of the ethash PoW chain and to ramp up gradually towards “pure” PoS.
- Given the significant increase in ETH network value, this gradual transition to PoS is a prudent strategy to prevent potential value destruction while transitioning a significant piece of the underlying Ethereum infrastructure.



FFG vs TFG

A Tale of Two Caspers

- Casper is not a specific implementation but a family of two main projects under active research by the Ethereum team.
- The Friendly Finality Gadget (“FFG”)—aka “Vitalik’s Casper”—is a hybrid PoW/PoS consensus mechanism, which is the immediate candidate for Ethereum’s first bridge to proof of stake. (PoS overlay on top of the ethash proof of work chain.)
- Casper the Friendly GHOST (“TFG”)—aka “Vlad’s Casper”—is a pure PoS proof of concept and will inform future iterations. Vlad’s work focuses on using a correct-by-construction approach to designing protocols. Extending local views of a node’s estimate of safety to achieve consensus safety is a key feature in particular.

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

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.

Agenda

- **What is Cryptoeconomics?**
- **Casper 101**
  - General PoS
  - Casper-specific
- **Latest Research** 👈🏼 🦄
  - Participation Constraint
  - CAPM & Sharpe Ratio
  - Liquidity & Opportunity Cost
  - Bayesian Games and Incomplete Information
  - Validator Slashing Trilemma

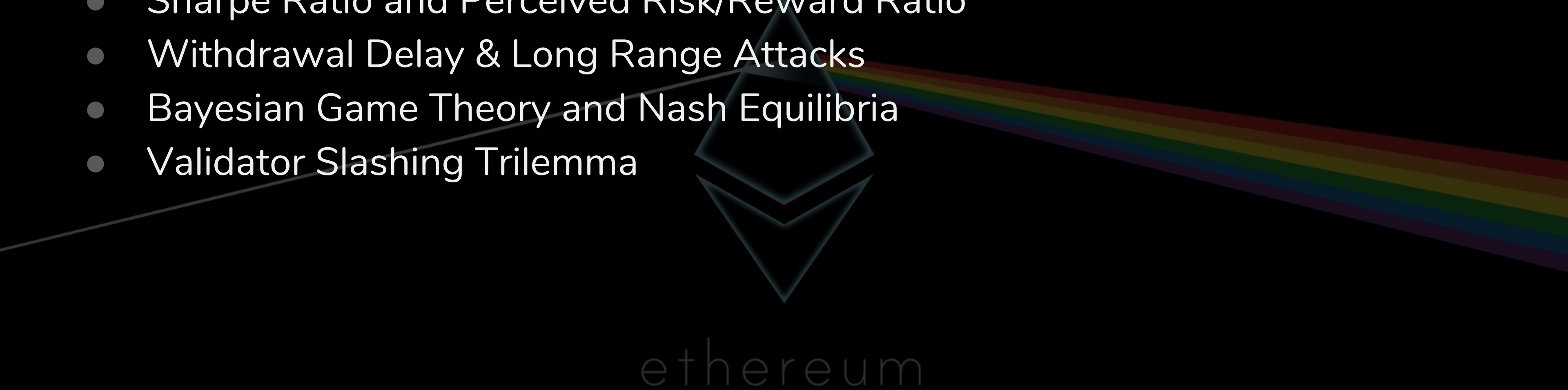
Latest Research

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

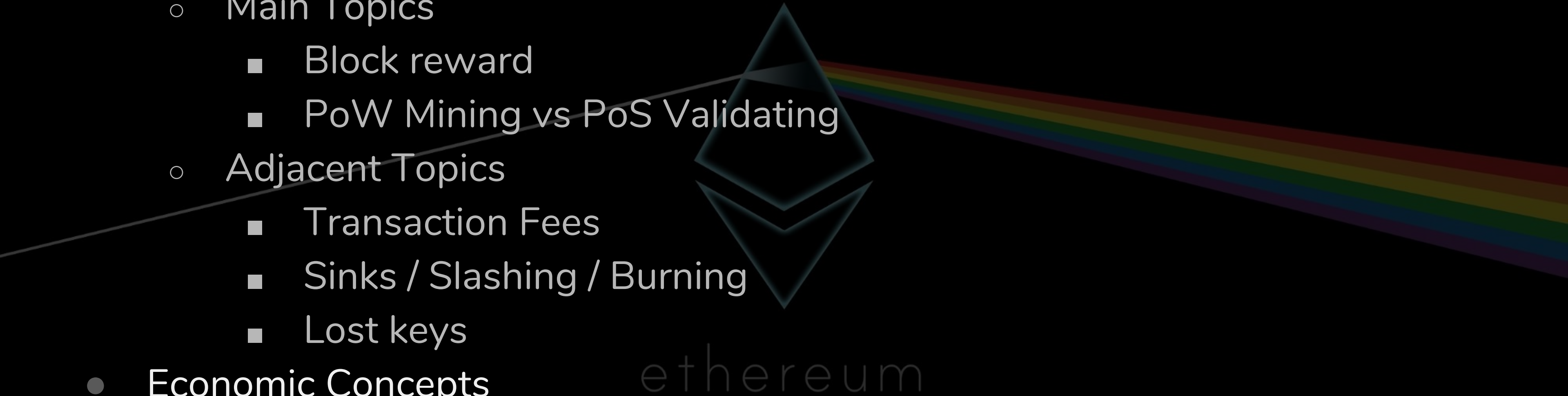
- Participation Constraint Analysis 👈🏼 🦄
- Sharpe Ratio and Perceived Risk/Reward Ratio
- Withdrawal Delay & Long Range Attacks
- Bayesian Game Theory and Nash Equilibria
- Validator Slashing Trilemma



What’s our budget?

What’s our budget?

- “Crypto” Concepts
  - Main Topics
    - Block reward
    - PoW Mining vs PoS Validating
  - Adjacent Topics
    - Transaction Fees
    - Sinks / Slashing / Burning
    - Lost keys
- Economic Concepts
  - Quantity Theory of Money
    - Inflation



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

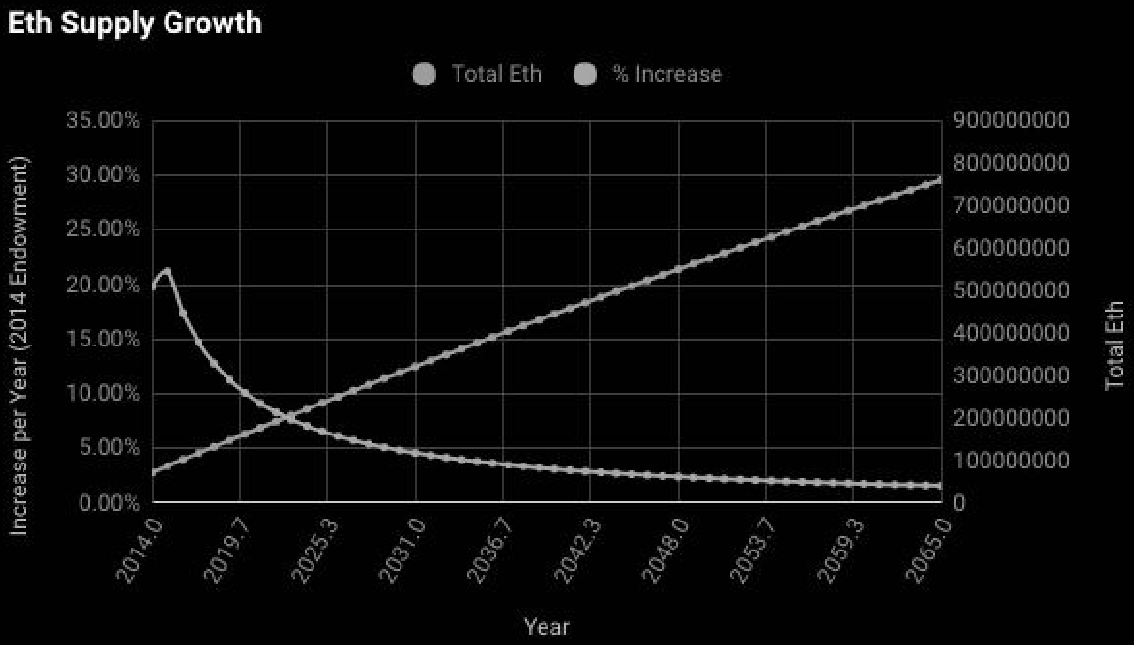
Credit: Wikipedia

Inflation

- 2017 inflation on target for [~15%]
  - US inflation is ~2% today (LTM).
  - BTC is at 4.3% (15% in late 2013)
  - Future
    - In ten years, ~6%
    - In twenty years, 3.5%

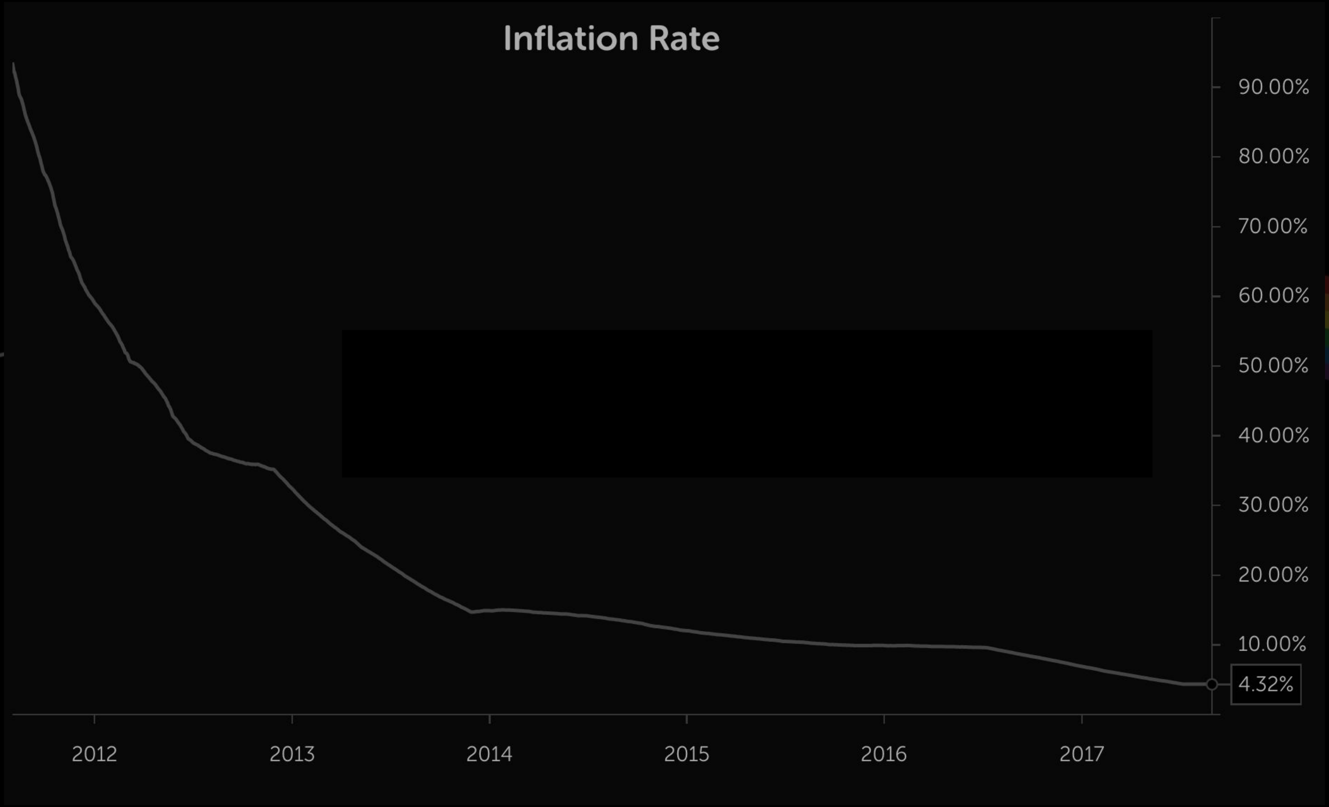
Ethereum Inflation Rate

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



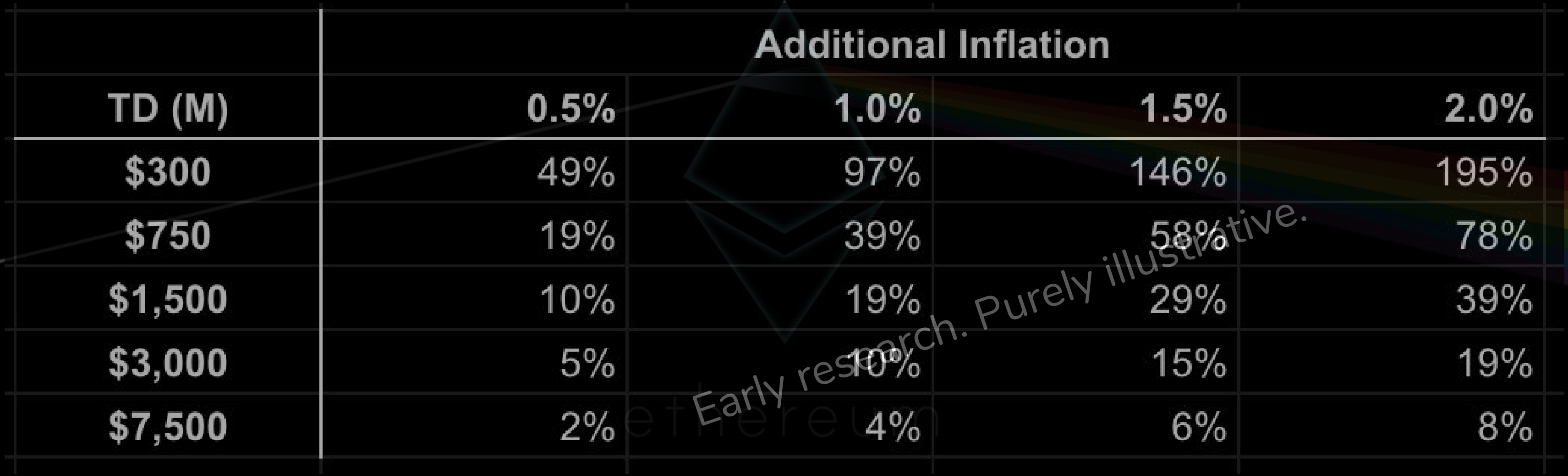
Credit: Joseph Lubin blogpost

How about for Bitcoin?



[redacted]

Illustrative Validator Yield Ranges



	Additional Inflation			
TD (M)	0.5%	1.0%	1.5%	2.0%
$300	49%	97%	146%	195%
$750	19%	39%	58%	78%
$1,500	10%	19%	29%	39%
$3,000	5%	10%	15%	19%
$7,500	2%	4%	6%	8%

Early research. Purely illustrative.

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 👈🏼 🦄
- Withdrawal Delay & Long Range Attacks
- Bayesian Game Theory and Nash Equilibria
- Validator Slashing Trilemma

Will people choose to participate?

Participation Constraint & Required Return

- “Crypto” Concepts
  - PoW Mining vs PoS Validating
  - Byzantine Fault Tolerant Consensus Protocols
- Economic Concepts
  - Participation / Budget Constraint
  - Utility
  - Risk / Loss aversion
  - Cost of capital / Opportunity Cost
  - Time value of money / Discount rate
  - Sharpe Ratio, CAPM

Participation Constraint Analysis

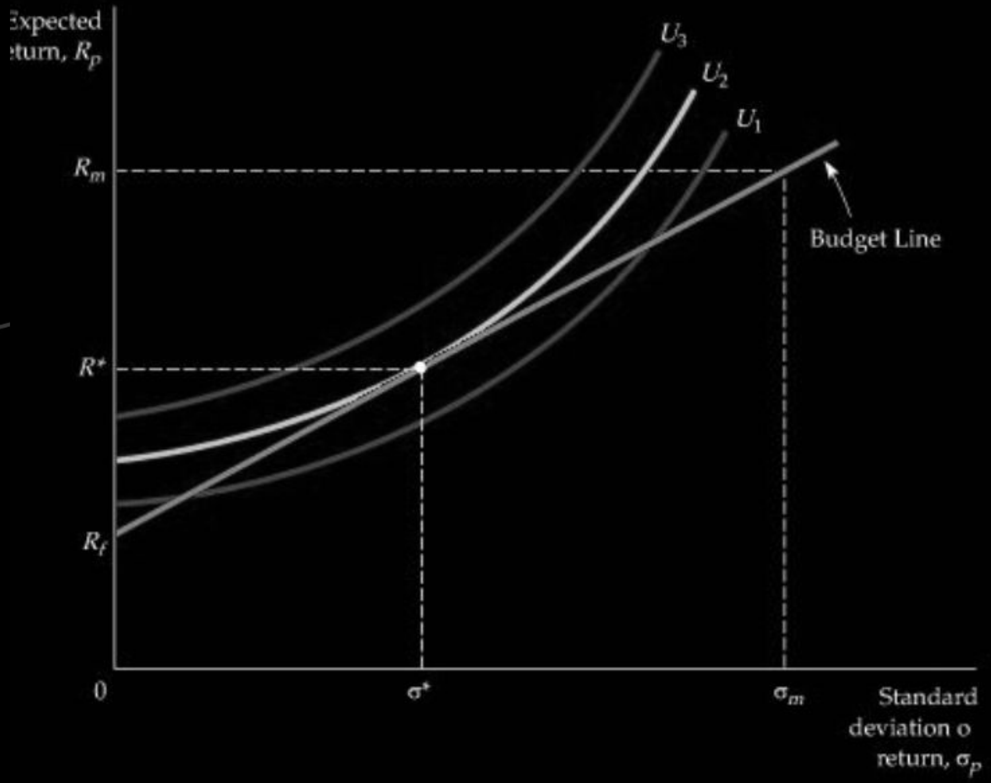
- “Will the mechanism be compelling enough for various validators to participate at all?”
  - Assuming that people will participate no matter what because “Ethereum is so great” is not acceptable
- Main Tradeoff: Issuance and average returns
- Design Consideration: Clearly communicating honest vs byzantine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

Risk Return Analysis

- CAPM
- Sharpe Ratio
- “PRR” Ratio

Credit: Prentice Hall 2008

Risk Return Analysis



Credit: Prentice Hall 2008

CAPM & Sharpe Ratio

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

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

- 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.
- The more we can limit the standard deviation of validation yield, the lower the required returns of the validators
- There is a direct cost to ETH holders for having high standard deviation validator returns
- R_m selection is tricky.
- Limitations: higher volatility of returns

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

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

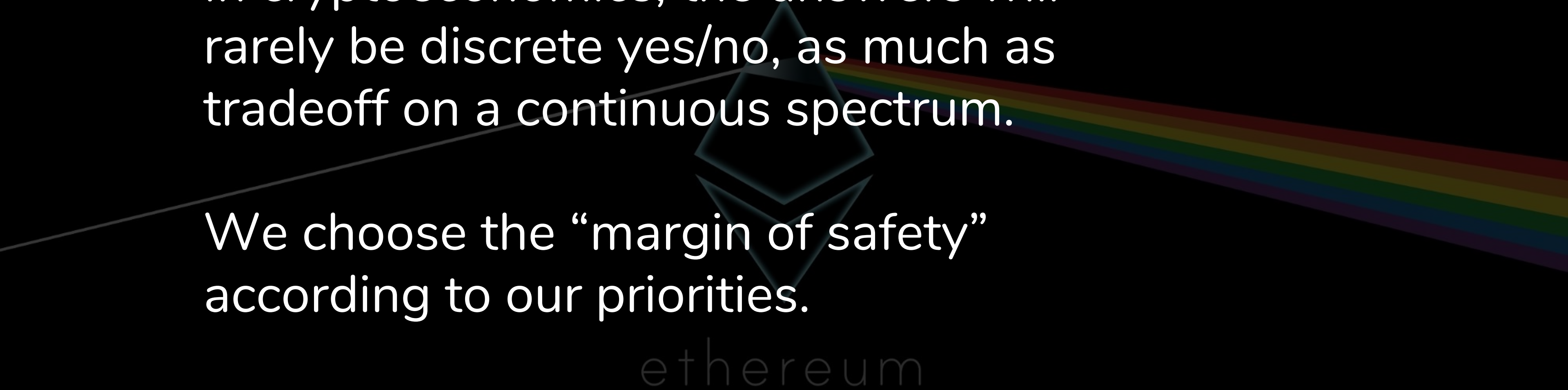
“Margin of Safety”

- Term comes from value investing.
- How much buffer do you have from the desired property?
  - Finance: how much below replacement cost can you buy real estate?
  - Cryptoeconomic security: how much total deposits needed?
  - Validator participation: how compelling is it to risk money to validate?
- 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 (topic for another day)

Credit: Seth Klarman

In cryptoeconomics, 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.



Economic Research Areas

- Participation Constraint Analysis
- Sharpe Ratio and Perceived Risk/Reward Ratio
- Withdrawal Delay & Long Range Attacks 👈🏼🦄
- Bayesian Game Theory and Nash Equilibria
- Validator Slashing Trilemma

Liquidity & Value

Liquidity & Value

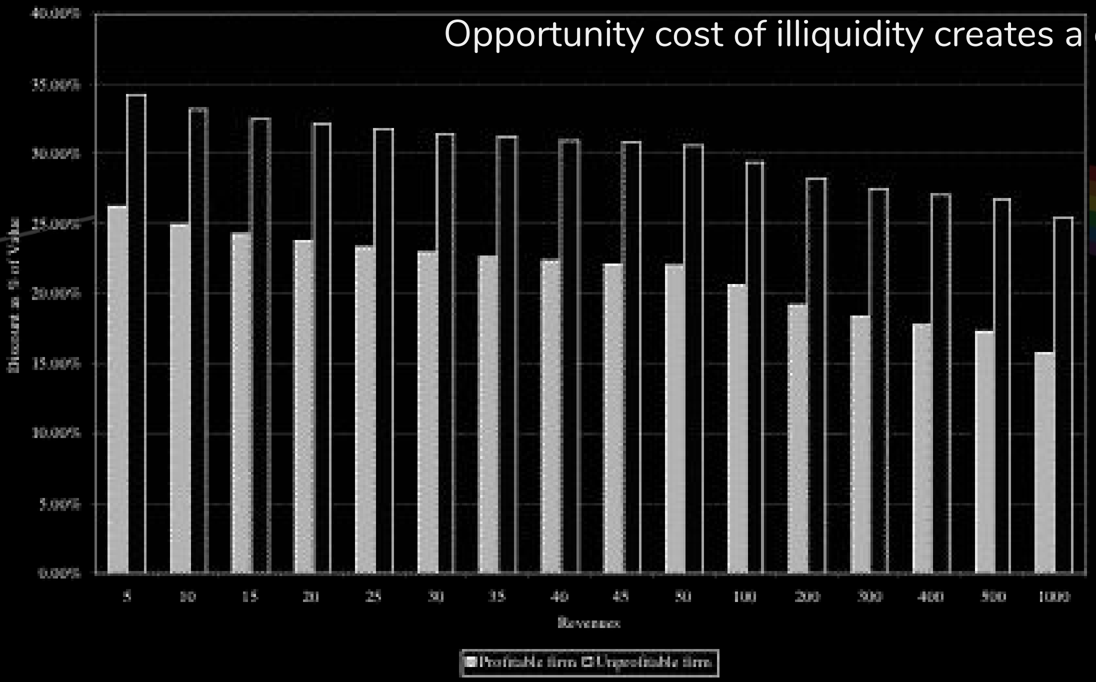
- “Crypto” Concepts
  - “Slasher” and deposit based PoS
  - Withdrawal Delays
- Economic Concepts
  - Liquidity (LAPM)
  - Opportunity Cost
  - Risk aversion / Loss aversion

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)

Withdrawal Delay

Figure 24.1: Illiquidity Discounts: Base Discount of 25% for profitable firm with $ 10 million in revenues



Opportunity cost of illiquidity creates a discount

Credit: Damodaran, NYU Stern

Economic Research Areas

- Participation Constraint Analysis
- Sharpe Ratio and Perceived Risk/Reward Ratio
- Withdrawal Delay & Long Range Attacks
- Bayesian Game Theory and Nash Equilibria 👈🏼 🦄
- Validator Slashing Trilemma

Bayesian Game Theory:
How others affect one’s decision?

Staking pools. Miners vs Stakers

- “Crypto” Concepts
  - Mining pools, Staking pools
  - Hybrid PoS/PoW
- Economic Concepts
  - Bayesian Game Theory
  - Incomplete Information Games
  - Common Prior Assumption
  - Single vs Iterated Games
  - Fixed Income Assets

Bayesian Games

- In game theory, a Bayesian game is a game in which the players have incomplete information on the other players (e.g. on their available strategies or payoffs), but, they have beliefs with known probability distribution.
- Validators will form their own view of what percentage of validators are Byzantine at any given point and the consequent impact on the yield of validating.
- It is also the role of the mechanism designer & community leader to (1) incentivize a healthy validator set mix but also (2) to maintain a healthy expectation around the validator set (much like the role of a central bank around interest rates).

Credit: Wikipedia

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

- While we cannot directly bound the amount of benefit attackers can have outside of the protocol, we can prepare for how damaging this attack vector can be at any point by being aware of:
  - (1) our own TD/MCap target (TD is the only direct way under our control to decrease ulterior factor, We want each “attack dollar” to have a lower multiple for affecting the market capitalization of ETH.)
  - (2) how certain competitors may be anti-correlated with ETH price and look to directly benefit from our potential failures.
- Relatively speaking, as the network’s TD level matures to the ideal levels, griefing factor matters more and ulterior factor matters less. So, during bootstrapping, ulterior factor is perhaps the largest liability (especially for an overlay on top of a “large cap” network).

“Fixed Income Approach”

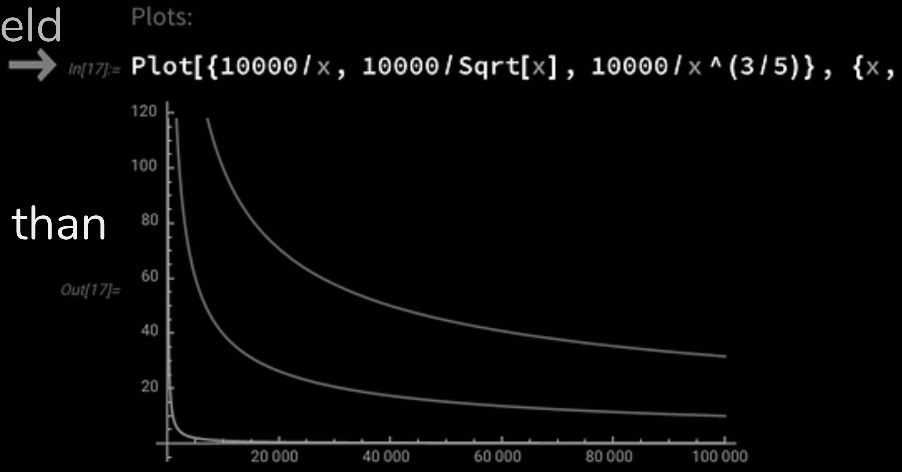
- In a fixed income asset, there’s a fixed amount of income that is paid out in regular intervals.
- Any qualifying actor can choose to participate or leave the mechanism, which determines the yield (income as a % of deposits) of the participants.
    - The more demand there is, the yield becomes competed away and becomes lower.
    - The less demand there is, the higher the yield becomes.

“Fixed Income Approach”

- Natural way for the market to determine the required return for a validator set.
- We can reversely incentivize a desired level of total deposits.
  - 1. Required Return as Determined by the Market
  - 2. Incentivizing a Total Deposit Level
  - 3. Total Deposits vs Market Cap

“Fixed Income Approach”: Limitations

- Tradeoff between certainty of issuance rate and mitigating game theoretic elements (i.e. selfish mining type behavior)
  - In a purely fixed income approach, your peers actions directly affect your yield dollar for dollar.
- Income / deposit vs income / deposit^x
- Robust over long periods of time rather than requiring frequent fine tuning.



Plots:

```
In[17]:= Plot[{10000/x, 10000/Sqrt[x], 10000/x^(3/5)}, {x,
```

Economic Research Areas

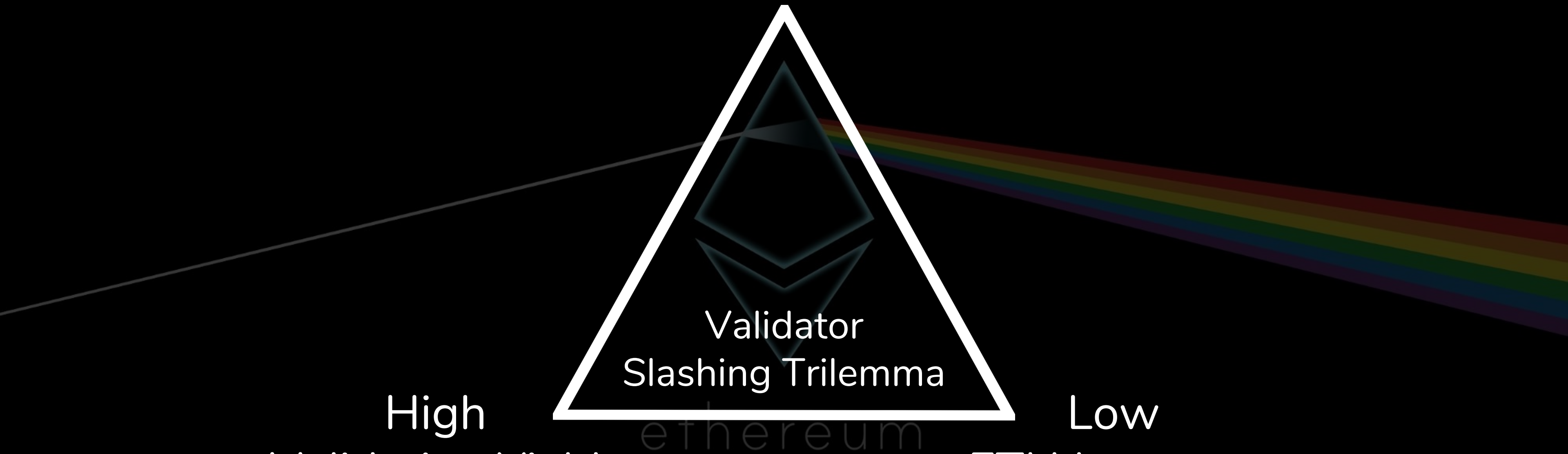
- Participation Constraint Analysis
- Sharpe Ratio and Perceived Risk/Reward Ratio
- Withdrawal Delay & Long Range Attacks
- Bayesian Game Theory and Nash Equilibria
- Validator Slashing Trilemma 👈🏼 🦄

Validator Slashing Trilemma

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

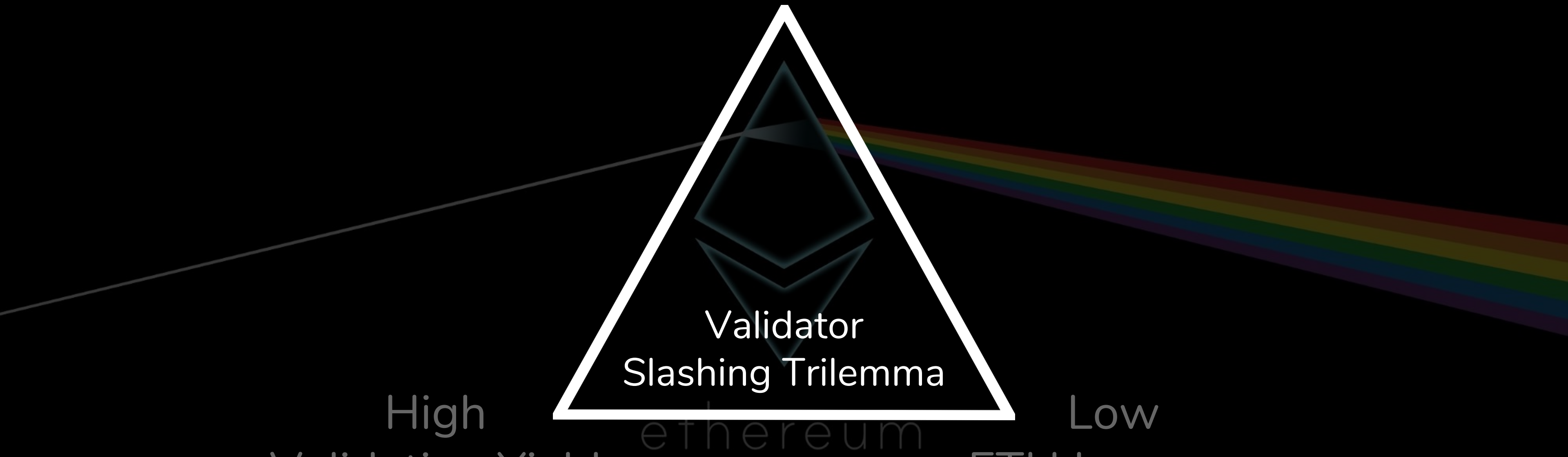


Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance

High
Cost of Attack

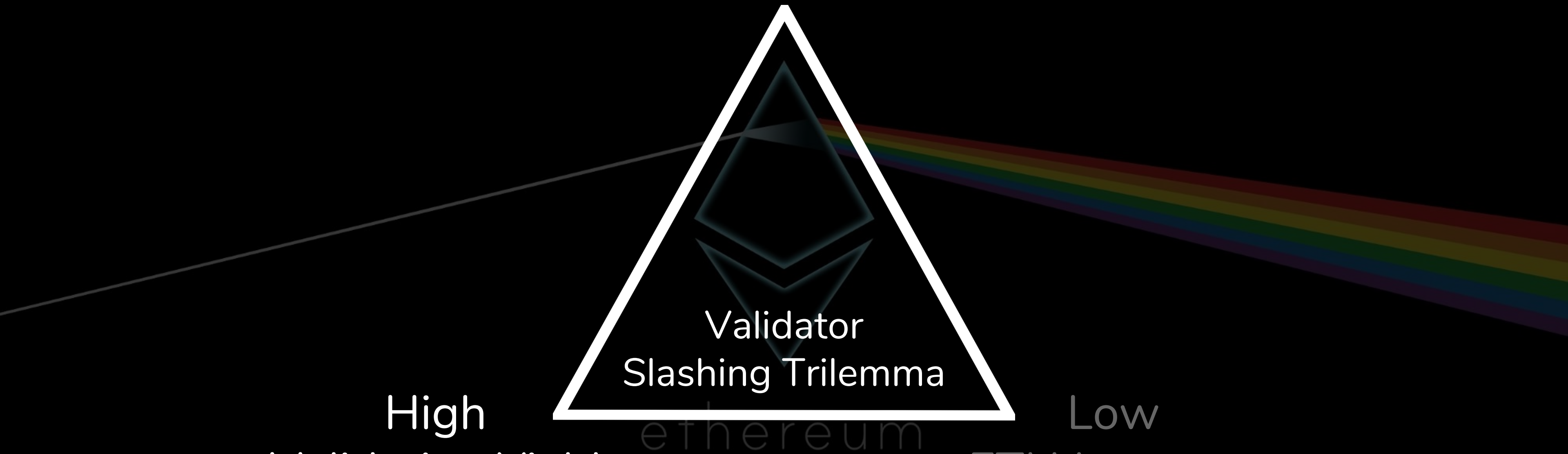


Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance

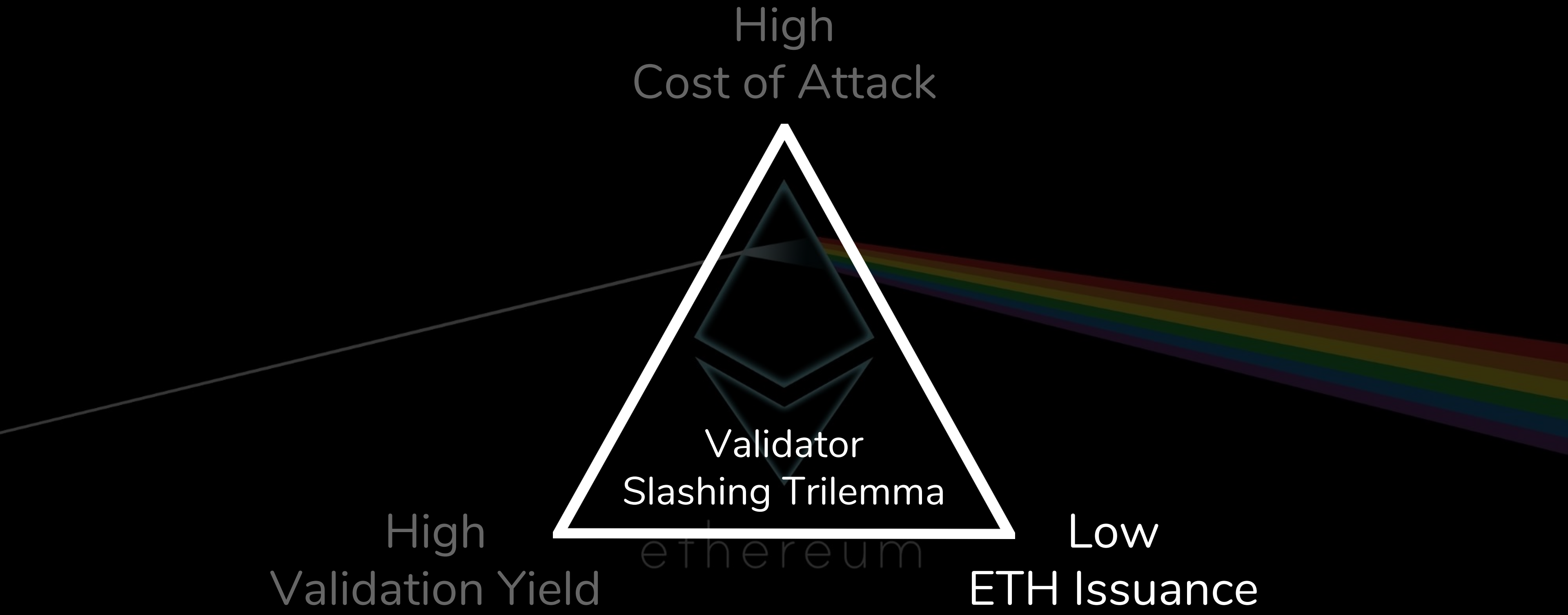
High
Cost of Attack



Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance



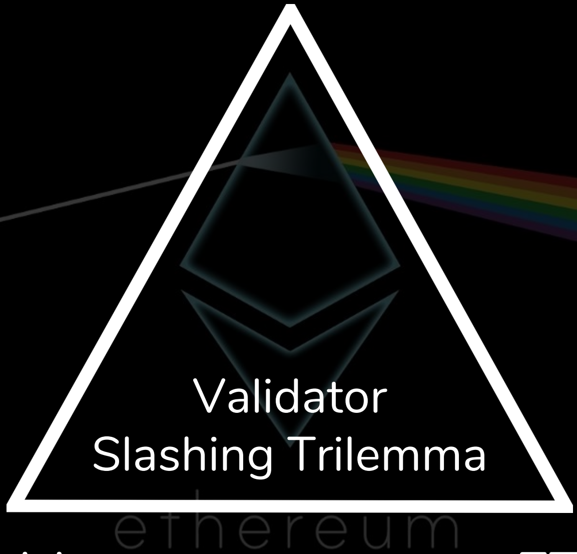
High
Cost of Attack

Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance

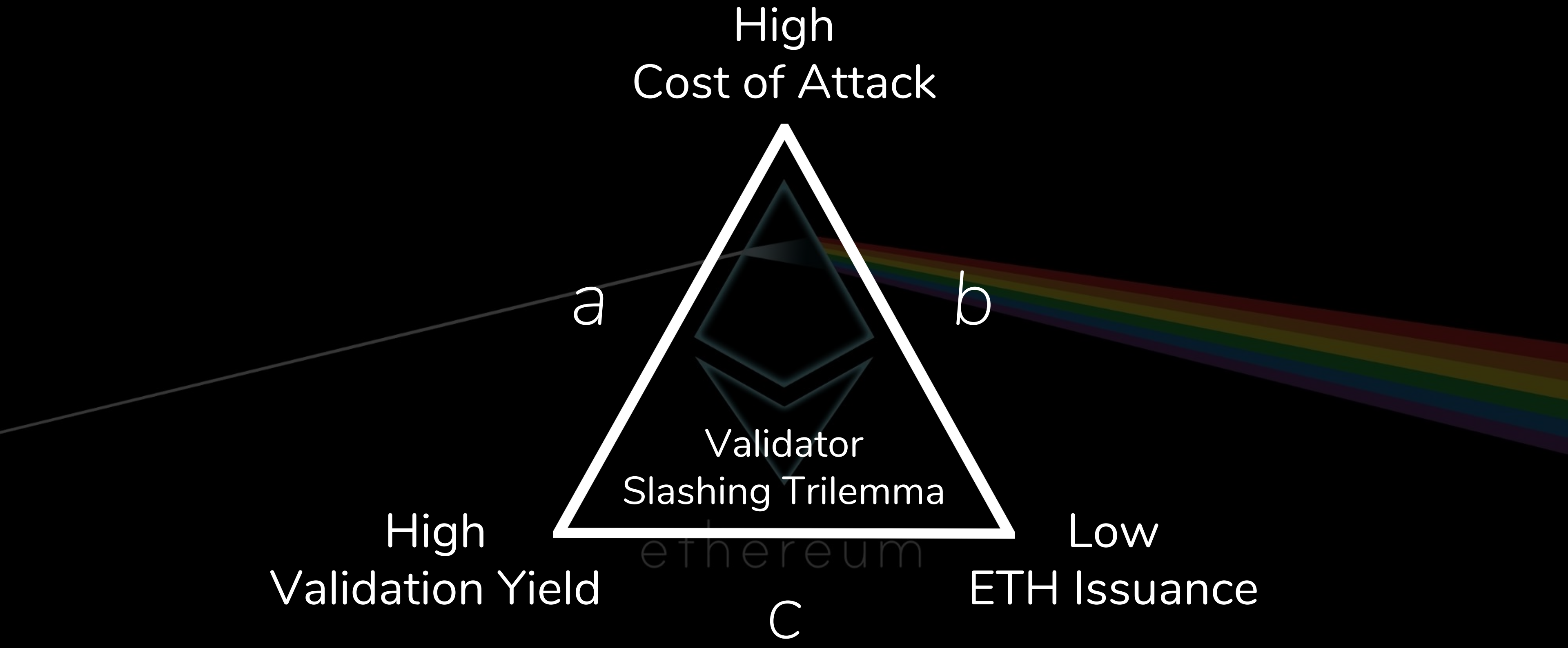
High
Cost of Attack



Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance



High
Cost of Attack

a

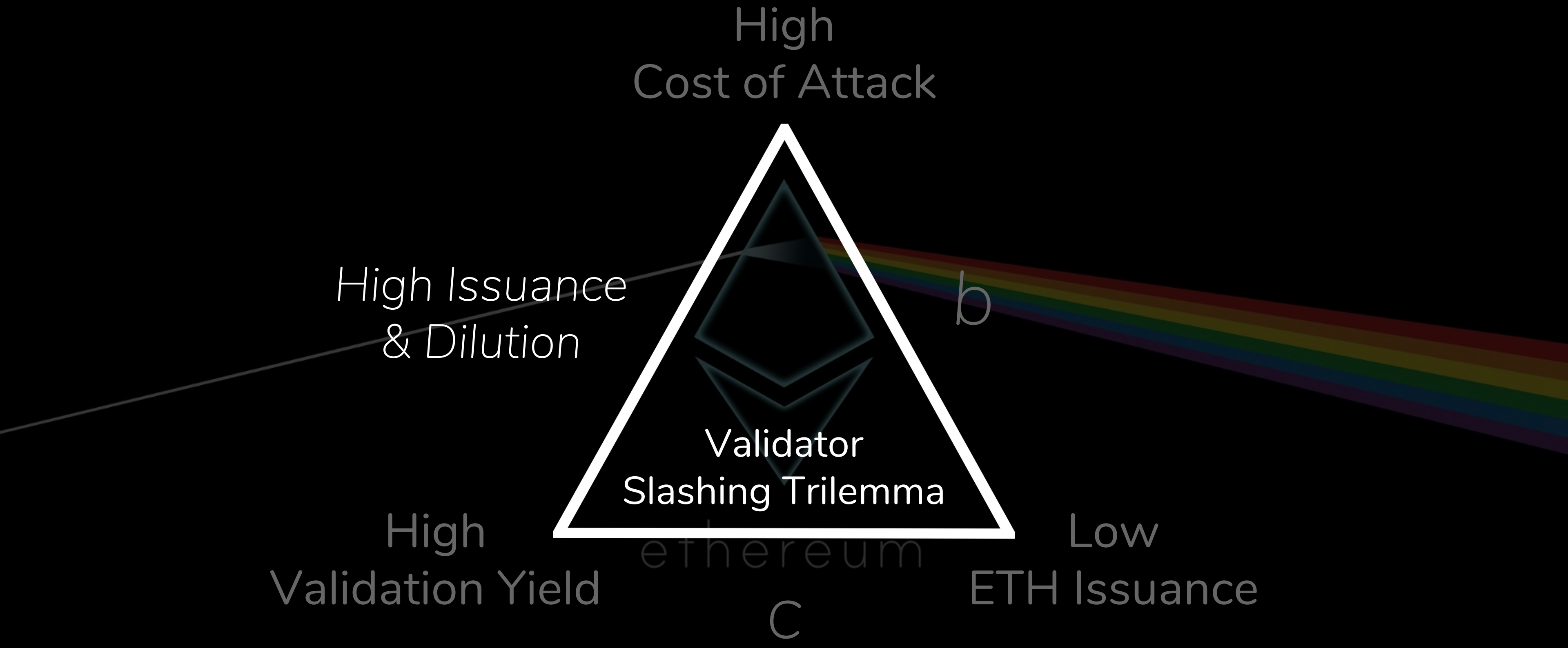
b

Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance

c



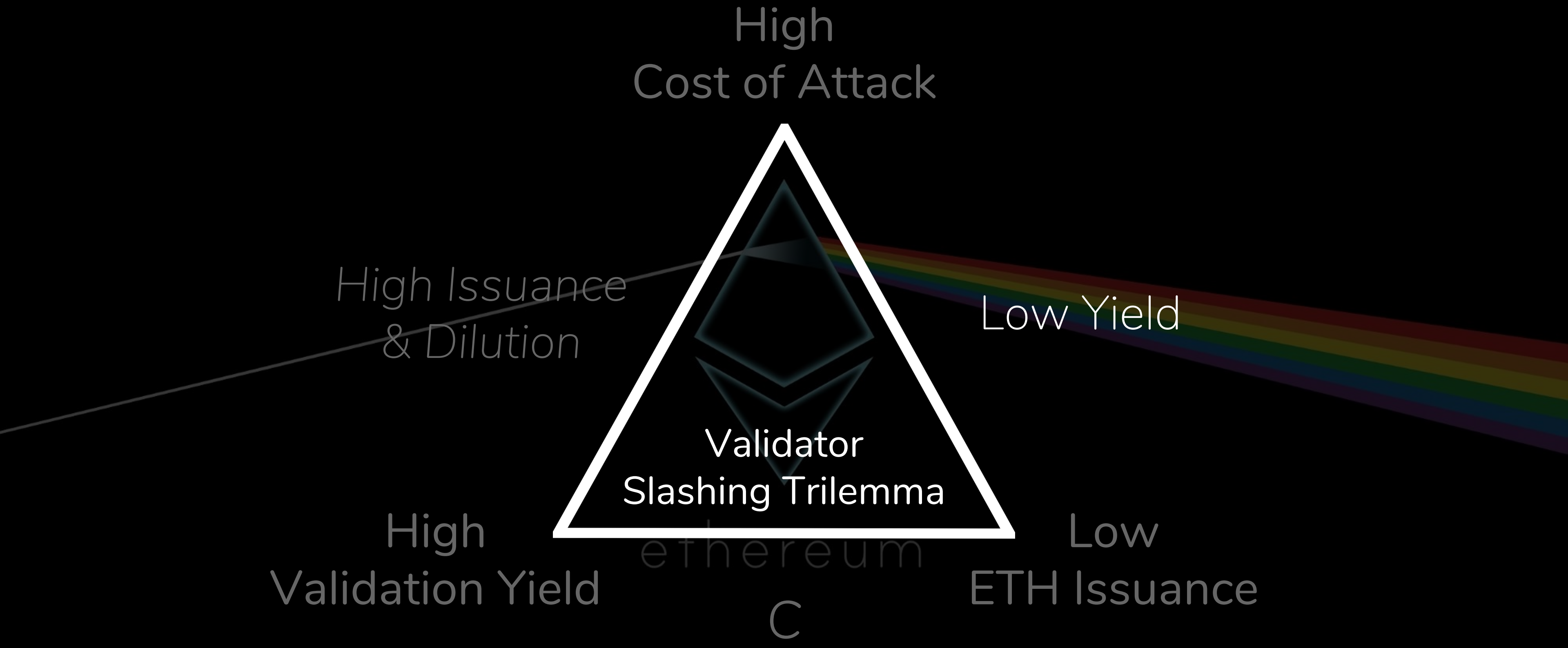
High
Cost of Attack

High Issuance
& Dilution

Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance



High
Cost of Attack

High Issuance
& Dilution

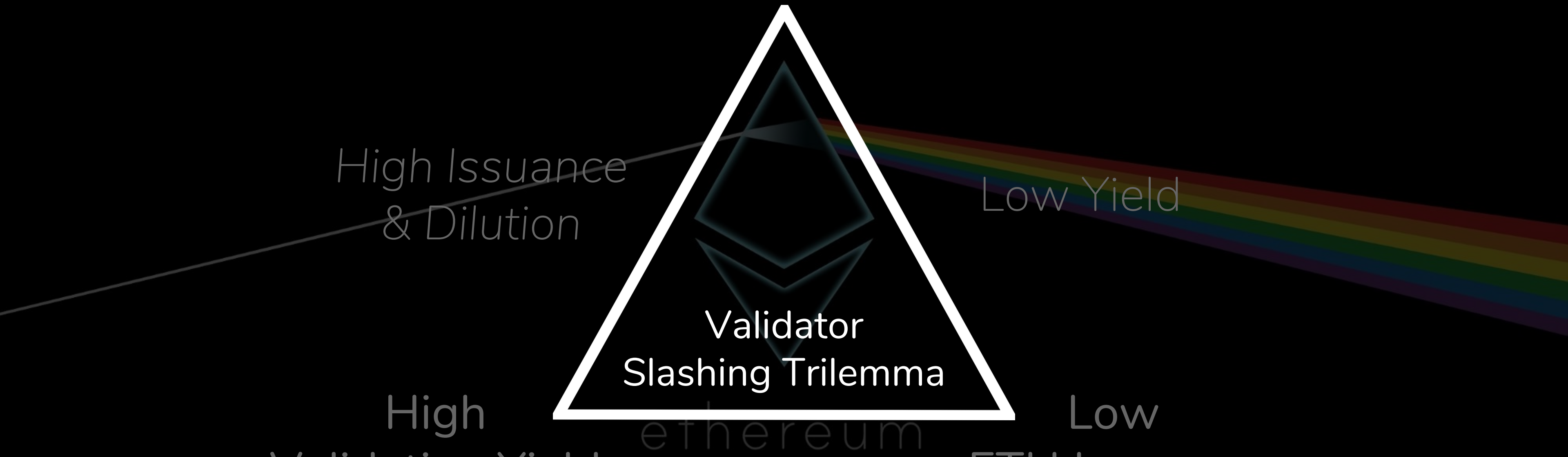
Low Yield

Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance

High
Cost of Attack



*High Issuance
& Dilution*

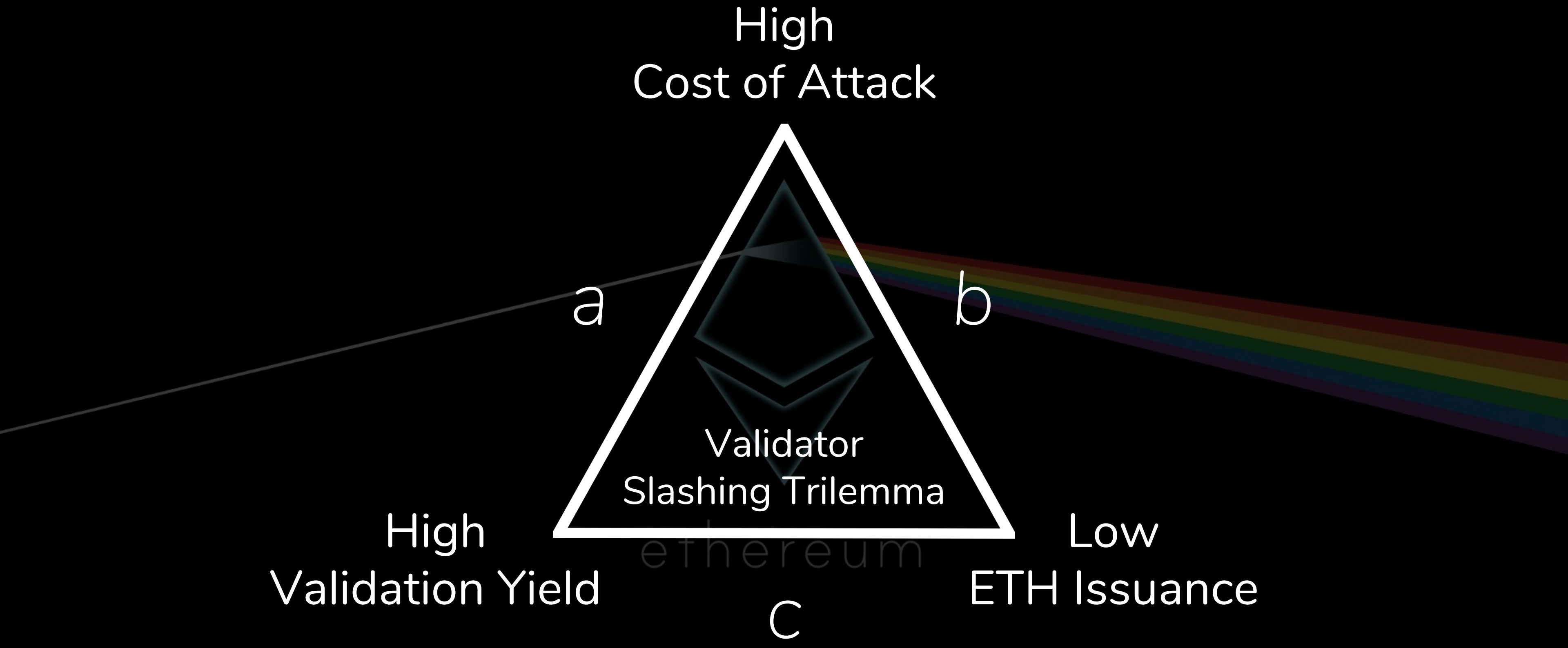
Low Yield

Validator
Slashing Trilemma

High
Validation Yield

Low
ETH Issuance

Less Draconian
Penalties



High
Cost of Attack

a

b

Validator
Slashing Trilemma

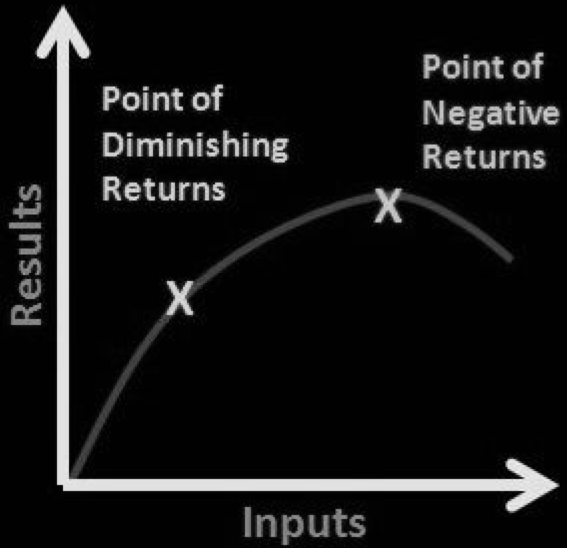
High
Validation Yield

Low
ETH Issuance

c

Econ Detour: Diminishing Marginal Returns

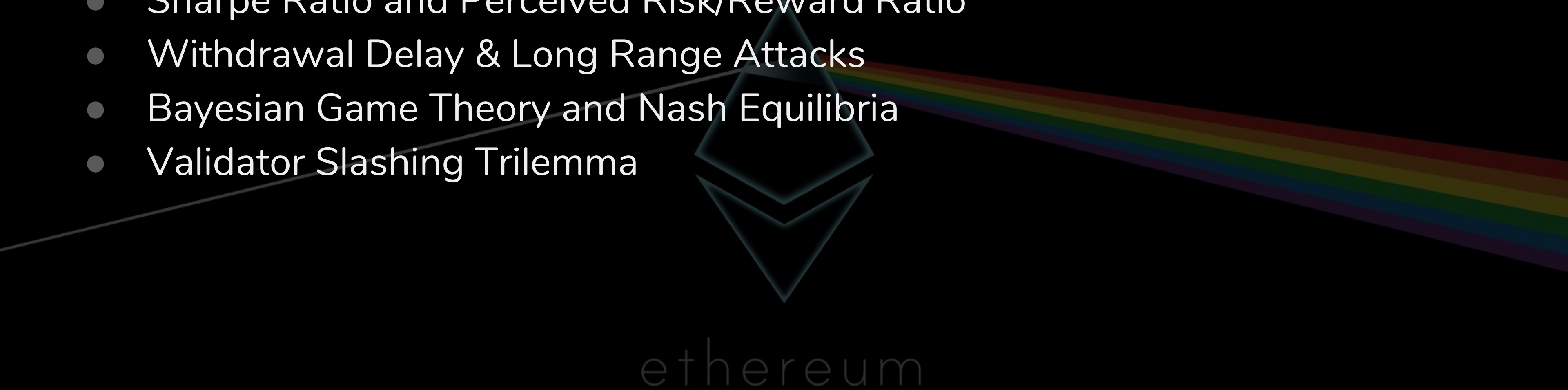
- Anecdote: real estate value. Trophy assets vs distressed assets.
- Example: Secret Service & the President. The marginal security added by each bodyguard.
    - Ultimately about how much security you need at what cost
- Takeaway: the highest cost of attack is not necessarily the optimal amount of security; 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

Economic Research Areas

- Participation Constraint Analysis
- Sharpe Ratio and Perceived Risk/Reward Ratio
- Withdrawal Delay & Long Range Attacks
- Bayesian Game Theory and Nash Equilibria
- Validator Slashing Trilemma



Future Work

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

To tie it all together…

Conclusion

- Cryptoeconomics is the study of secure transmission of digital scarcity in open networks.
- We want proof of stake for energy efficiency, proportional wealth distribution and fine-grained control over incentives.
- Casper has the benefits of PoS and further enables promising scaling solutions. Casper is being built from the ground up with incentives as a first-order design principle.
- We discussed the latest cryptoeconomic research that will be informing the parametrization and optimization of Casper.
- Please get in touch to learn more and contribute.

Parting thoughts

Cryptoeconomics is all about the subtle tradeoffs among desired properties.

There are great things that are OK at a certain price.

There are OK things that are great at a certain price.

Cryptoeconomics *noun*

The study of secure transmission of digital scarcity in open networks.

Thank you.

questions?
jonchoi.com

Q&A (if time allows)

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