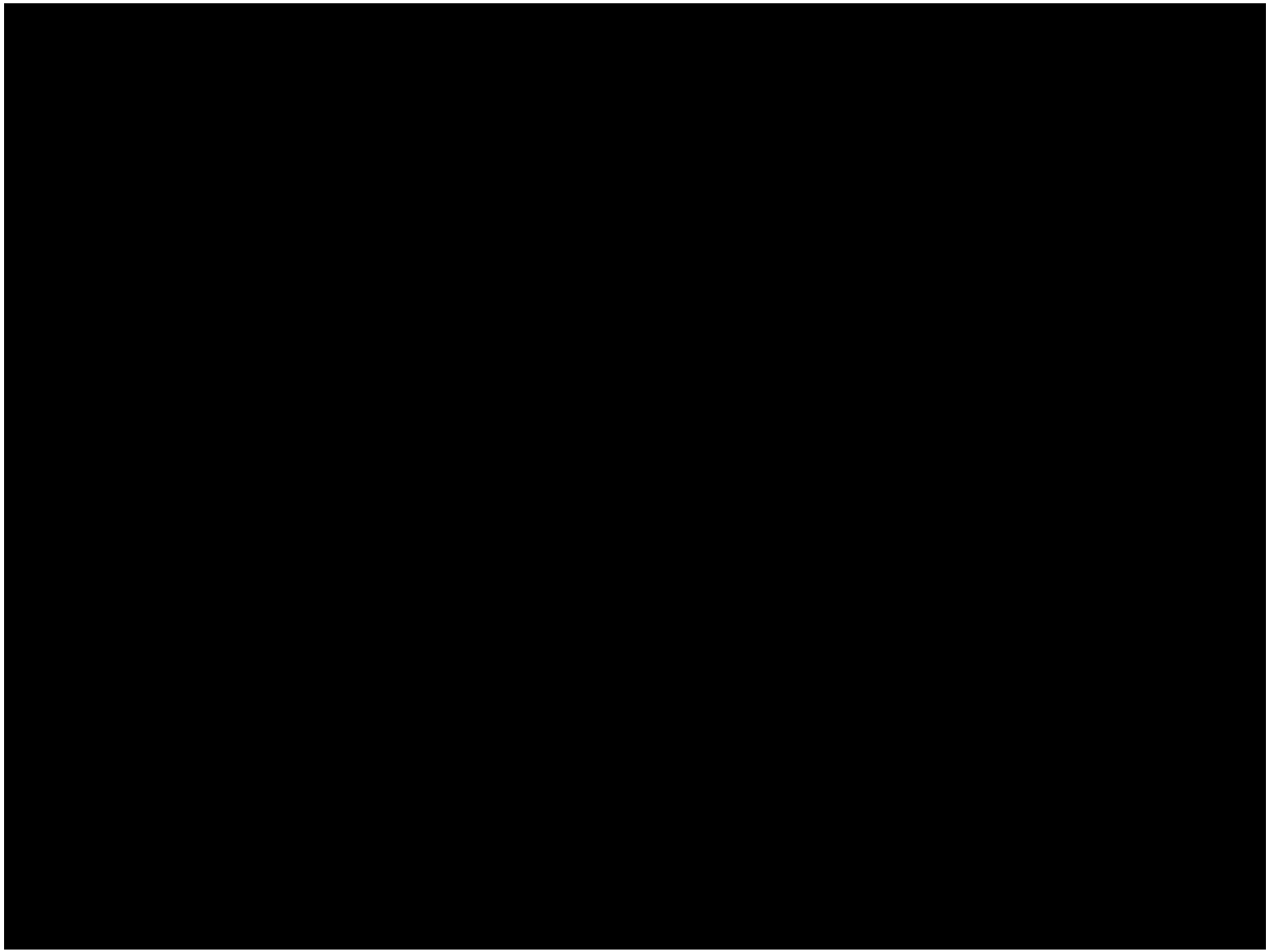
Blockchain Incentives

SMU LKCSB S3-10
26/10/2018



Bitcoin's incentives

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.

The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.

Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free. The incentive may help encourage nodes to stay honest.

If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth

Bitcoin's incentives

Decentralized currency

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.

The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.

Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free. The incentive may help encourage nodes to stay honest.

If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth

Bitcoin's incentives

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.

Mining

The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.

Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free. The incentive may help encourage nodes to stay honest.

If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth

Bitcoin's incentives

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.

The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.

Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free. The incentive may help encourage nodes to stay honest.

Security

If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth

What exactly are cryptoeconomic incentives?

	Confess	Don’t confess
Confess	(-6, -6)	(0, -10)
Don’t confess	(-10, 0)	(-1, -1)

A familiar example: Prisoners’ Dilemma

What exactly are cryptoeconomic incentives?

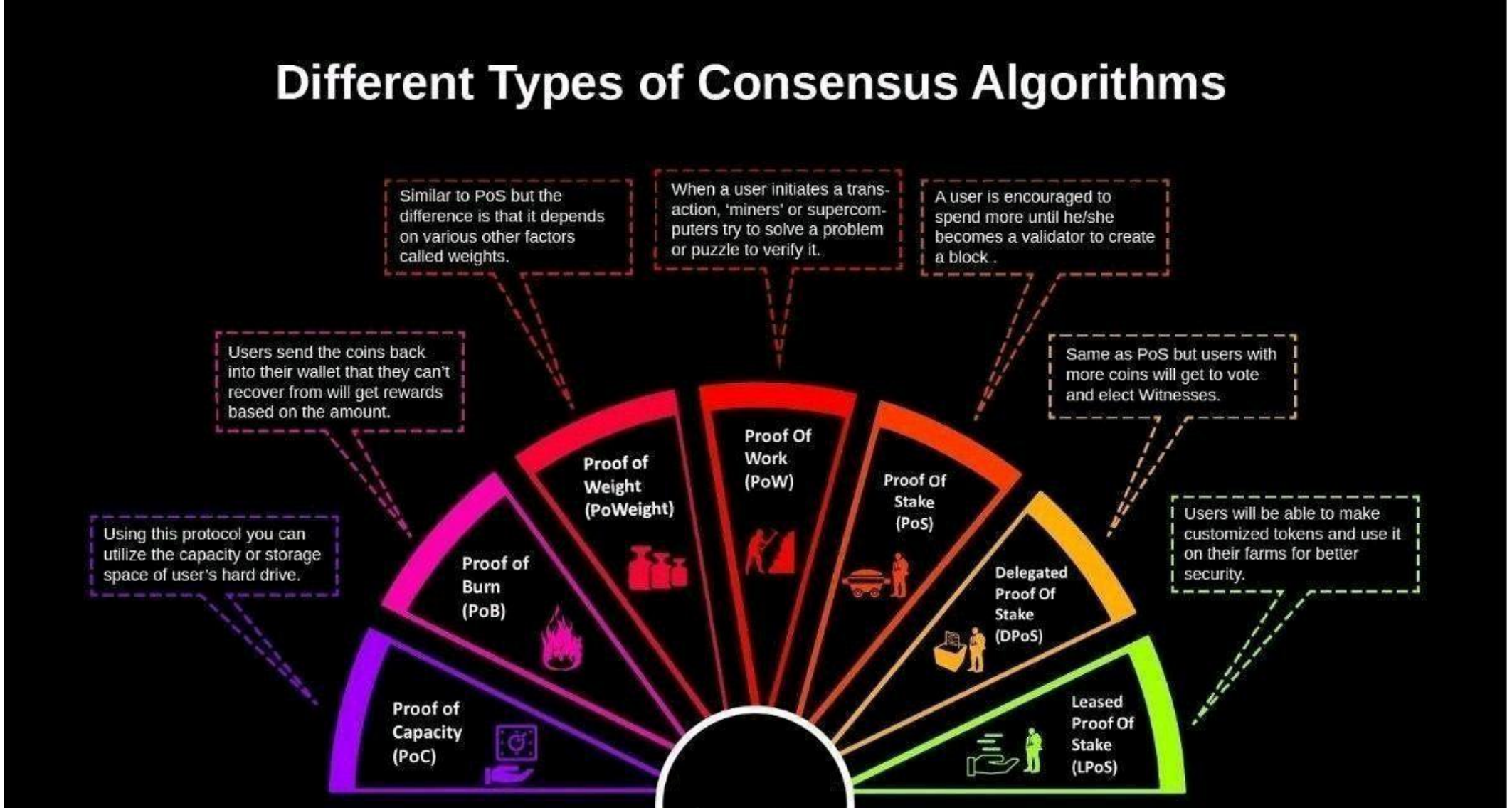
	Follow Protocol	Deviate
Follow Protocol	**Ideal**	(incentivize, punish)
Deviate	(punish, incentivize)	Just use AWS/GCP/AlibabaCloud

What exactly are cryptoeconomic incentives?

With added complexity of:

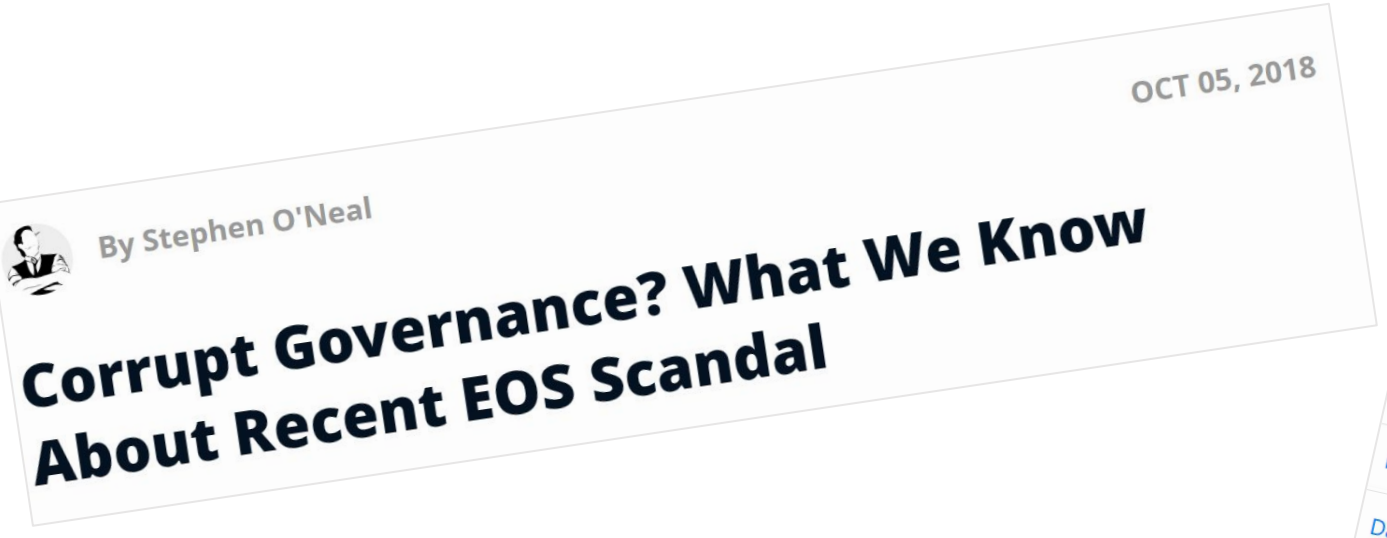
1. Cooperation/ collusion
2. Data accessibility/ protection
3. Transaction speed
4. Scalability
5. Real-world use of computational resources
6. Physics e.g. asynchrony

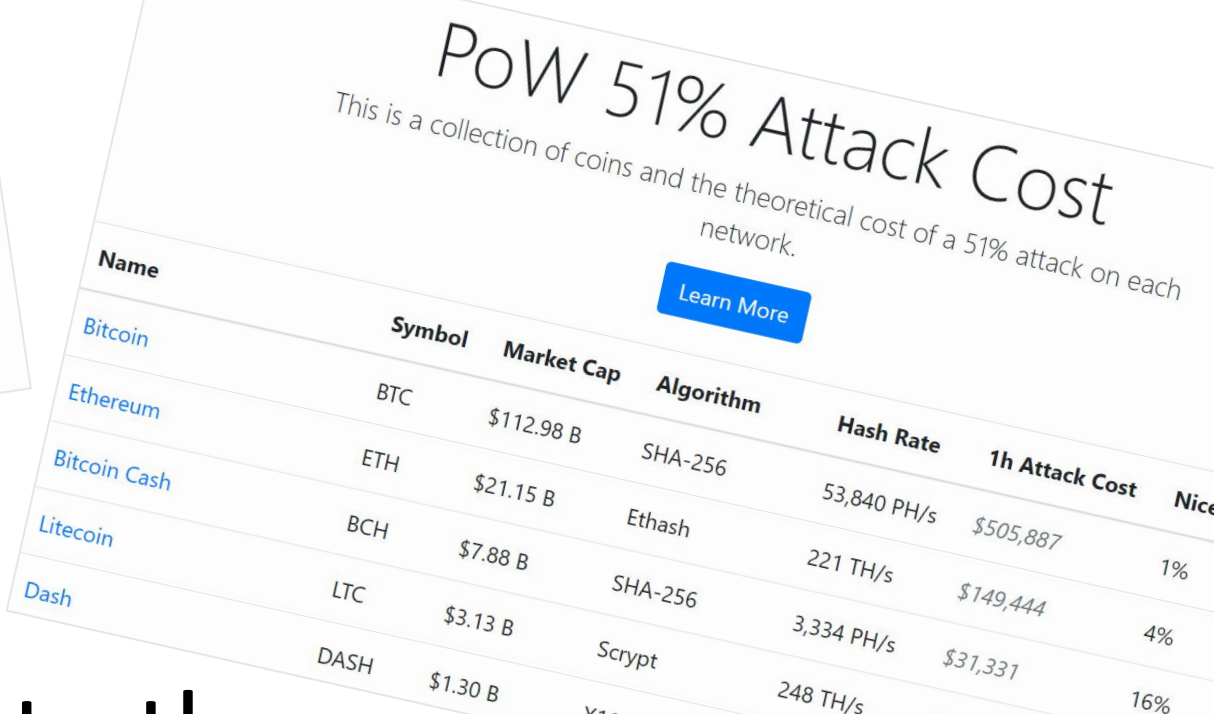
Name a Consensus Algorithm and why it is different from Bitcoin’s Proof-of-Work



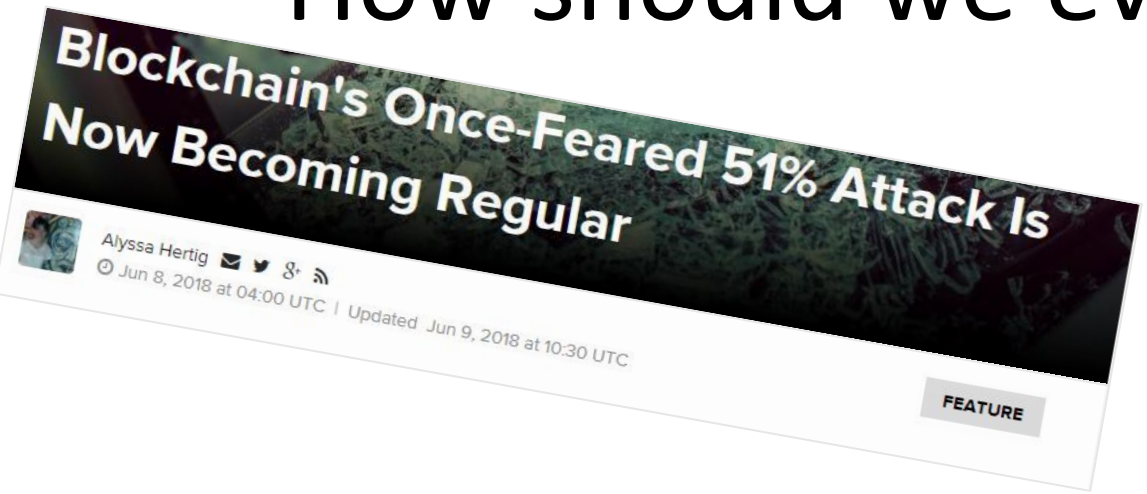
Created by 101blockchains.com

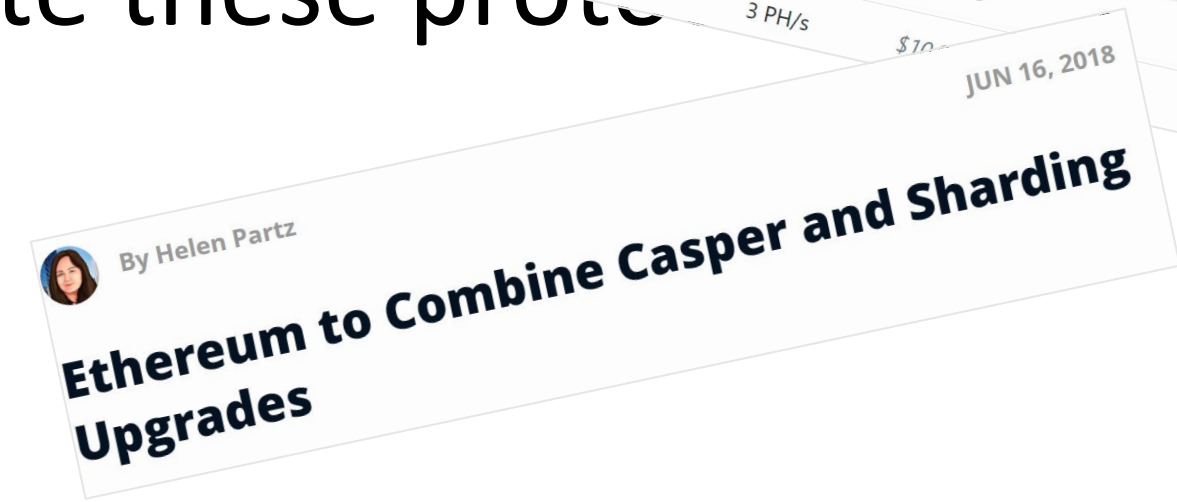
How should we evaluate these protocols?





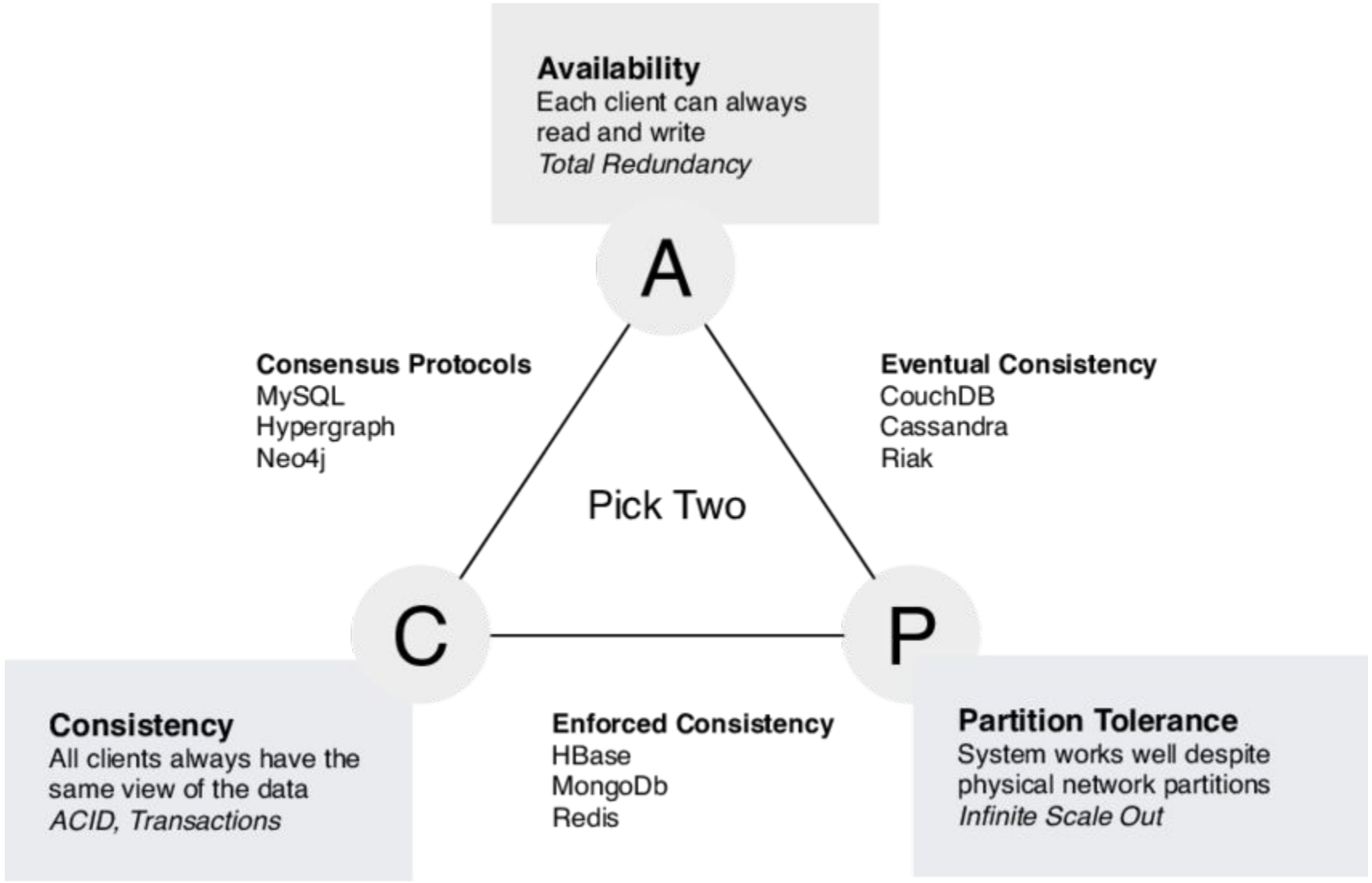
How should we evaluate these prote



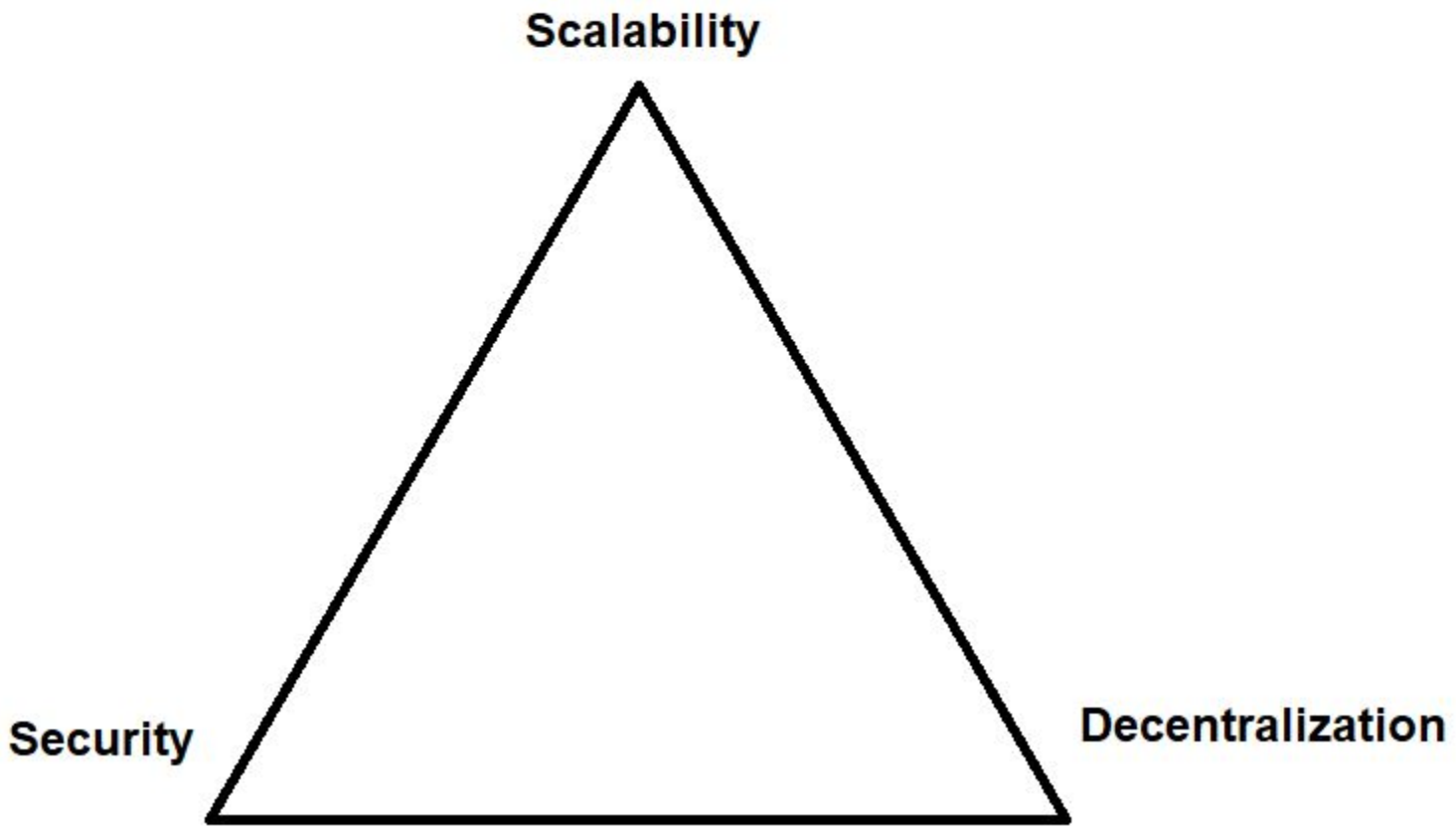


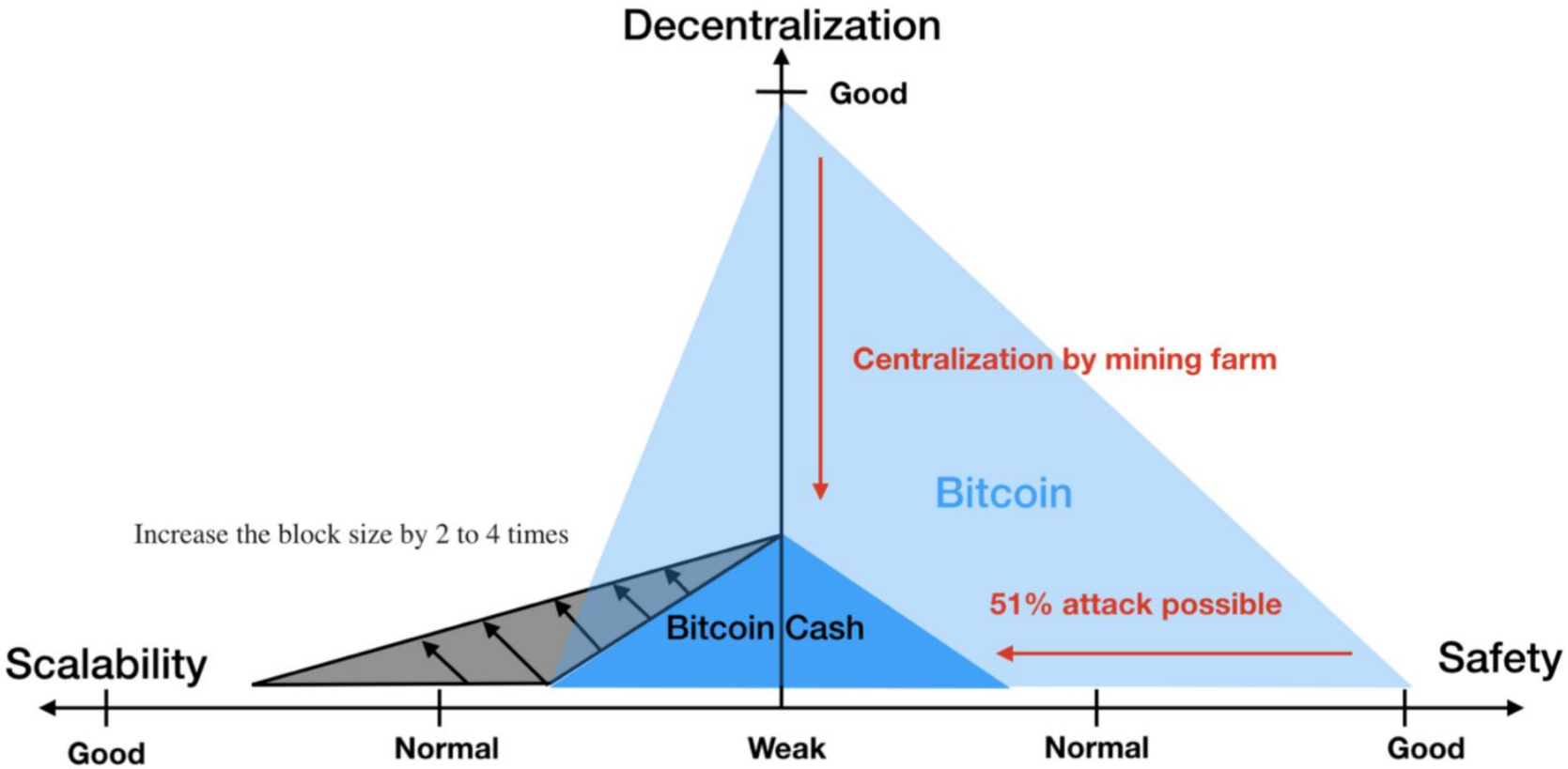
SWITCH

BLOCKCHAIN RESEARCH COLLECTIVE



The Blockchain Trilemma

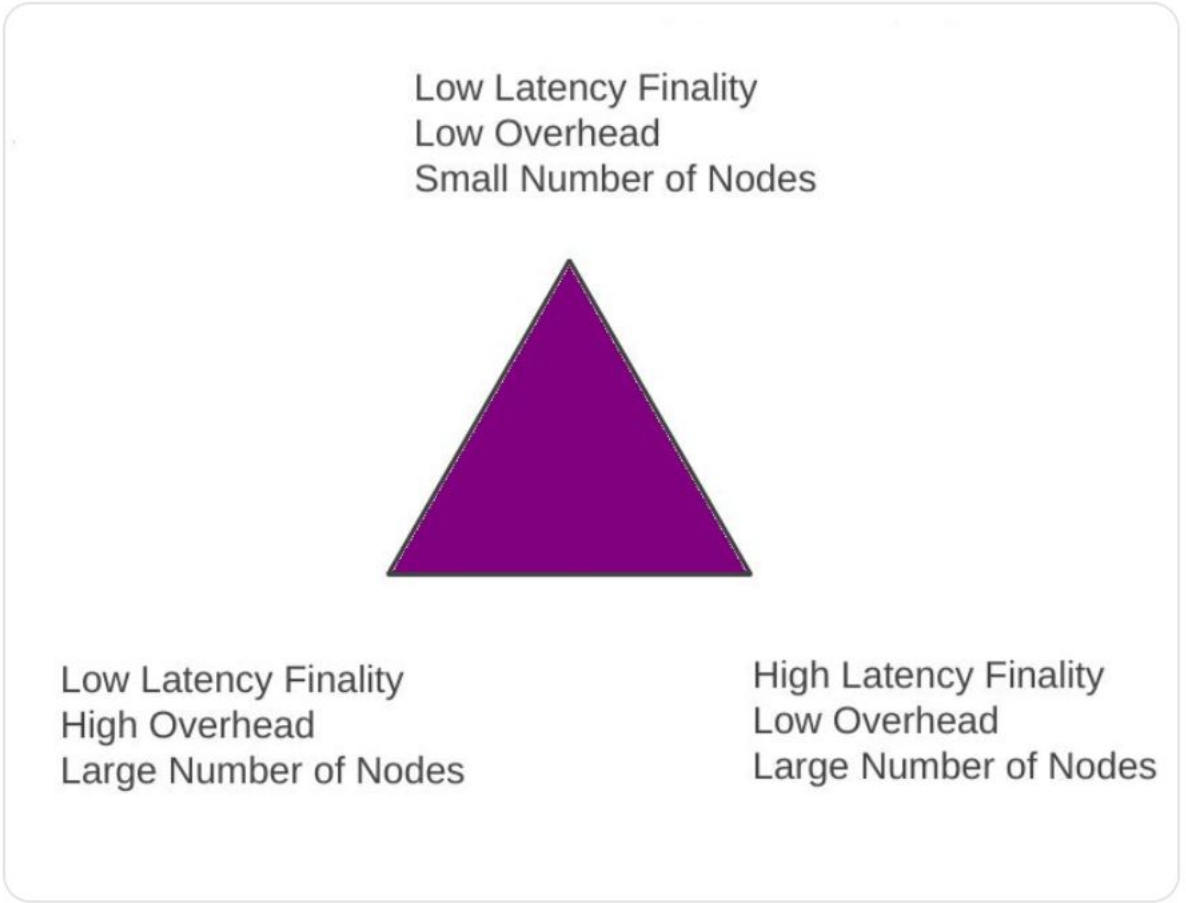




[그림 4. Bitcoin Cash's Trilemma]

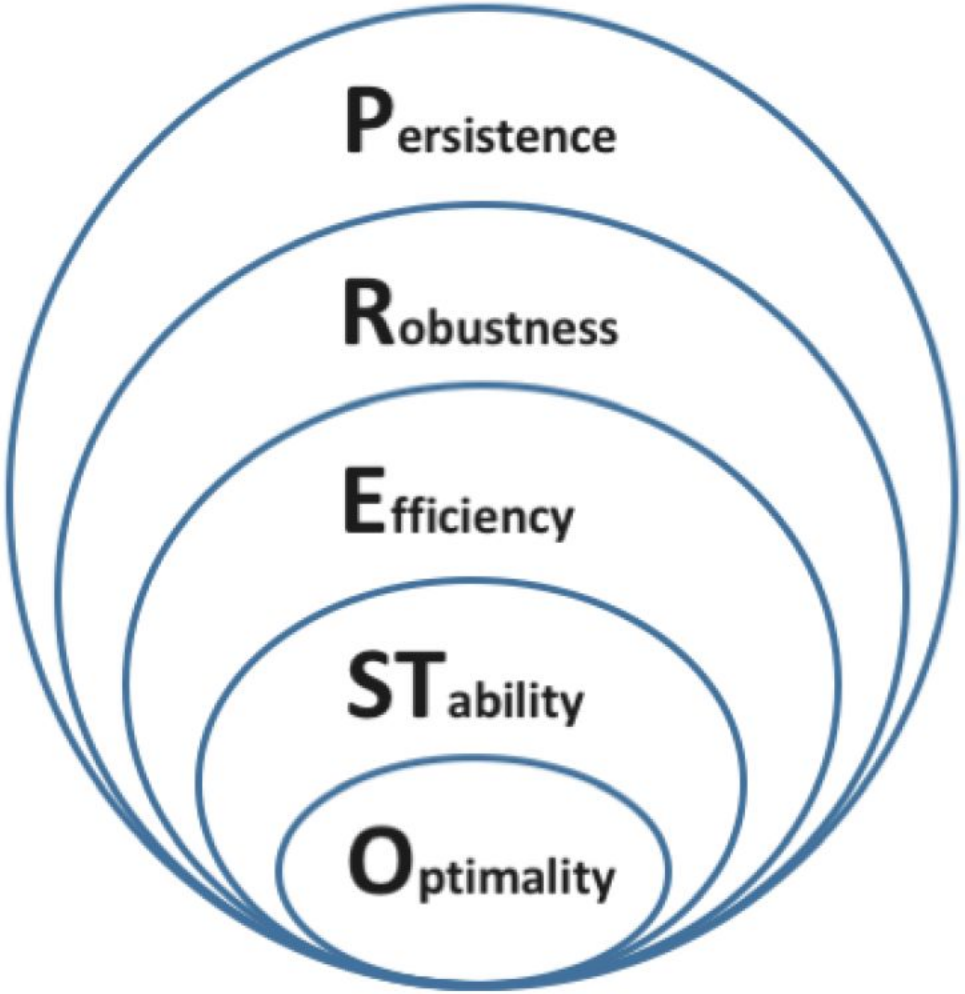
Vlad Zamfir @VladZamfir · 16 Dec 2017

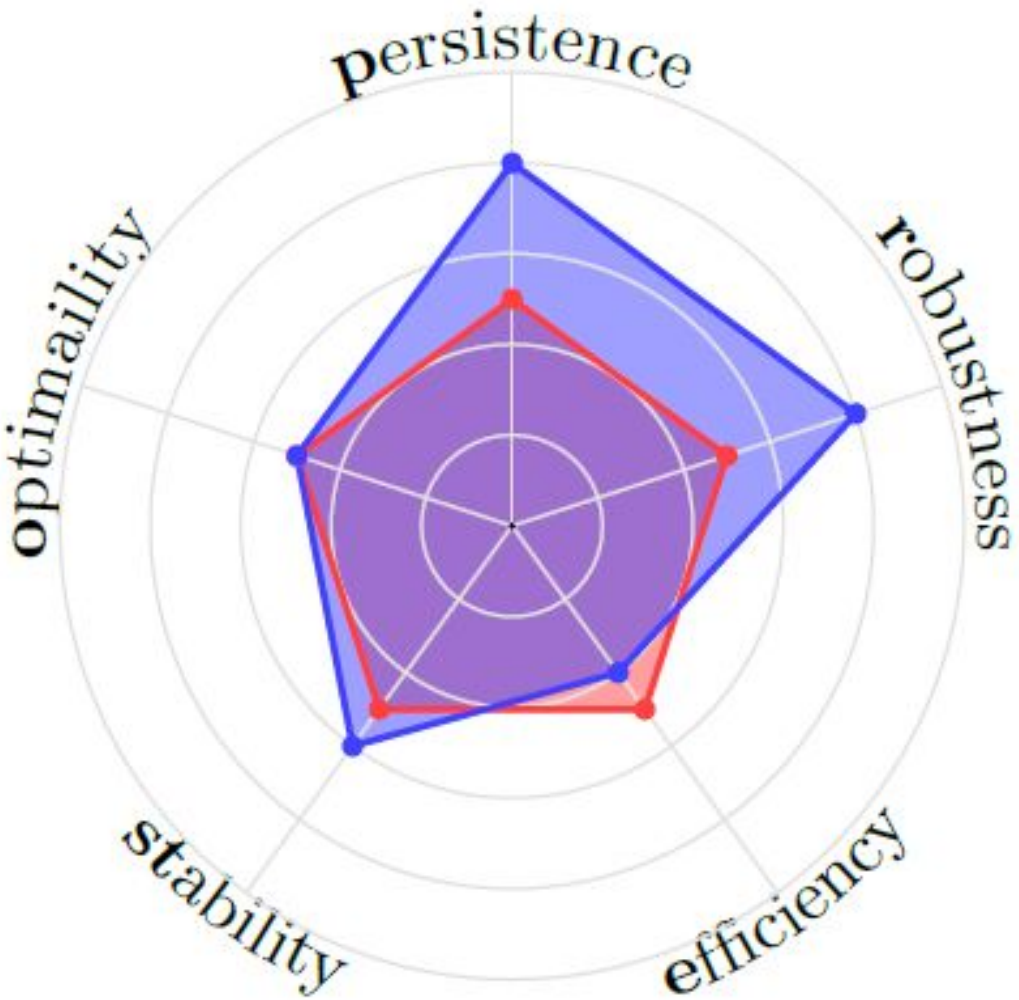
Casper the Friendly Ghost's parametrization, on the other hand, can explore the tradeoff space in all the directions!



3 7 50

There are still several dimensions that may affect the performance of blockchains in the wild


Persistence
Robustness
Efficiency
STability
Optimality


persistence
robustness
efficiency
stability
optimaility

PRESTO framework

Optimality: does the protocol provide the necessary distributed computation guarantees, i.e., guarantee safety and eventual liveness? In an ideal world where all agents faithfully implement the protocol, does it work as intended?

Stability: is it a Nash equilibrium to follow to protocol rather than engage in deviant behaviour such as block withholding?

Efficiency: what is the protocol's throughput relative to its usage of resources such as time, space, energy, and financial resources?

Robustness: does the protocol cope well when assumptions turn out to be invalid, e.g., when agents behave in a way that is not rational in terms of the protocol payoffs? In other words, how robust is the (Nash) equilibrium to perturbations of the agents' payoffs?

Persistence: can the protocol recover from serious attacks?

PRESTO Framework

- **Many** (>2000) different protocols (cryptocurrencies):
  - How do they differ? Which is “better”?
  - Already several **surveys** that try to compare them? **But how?**

- **P.R.E.ST.O:** A set of principles for effective design of sytems
  - In particular, **consensus protocols**
  - **Structured** & **systematic** way to design & evaluate a mechanism.

Optimality

- **What is the protocol aiming to achieve?**

Optimality

- **Liveness**

  Valid transactions are (eventually) processed (included in the public ledger)

Optimality

- **Safety/Consistency**

  All honest participants reach agreement (consensus) on the order and validity of the transactions

"Then, gentlemen, it is the consensus of this meeting that we say nothing, do nothing, and hope it all blows over before our next meeting."

Optimality

- **Safety/Consistency**

  All honest participants reach agreement (consensus) on the order and validity of the transactions

"It looks like we have a consensus."

Optimality

- **Anything else?**

  Anonymity, smart contract support, ...

Stability

- **Is it incentive compatible (Nash equilibrium) for rational agents to follow the protocol if everyone else does so?**
- **Recall:** no central authority to enforce correct behaviour

Stability

- **Incentives**

  The protocol provides reward mechanism to promote correct behaviour by all agents

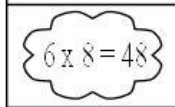
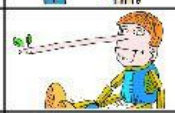
  - Participate
  - Perform operations:
    - include/validate transactions
    - propagate messages across the network
    - store data
  - Remain decentralized
  - Distribute profits fairly
  - …

Stability

- **Incentives**

  Recall: No central authority to enforce correct behaviour.

  All incentives must come from the protocol itself.

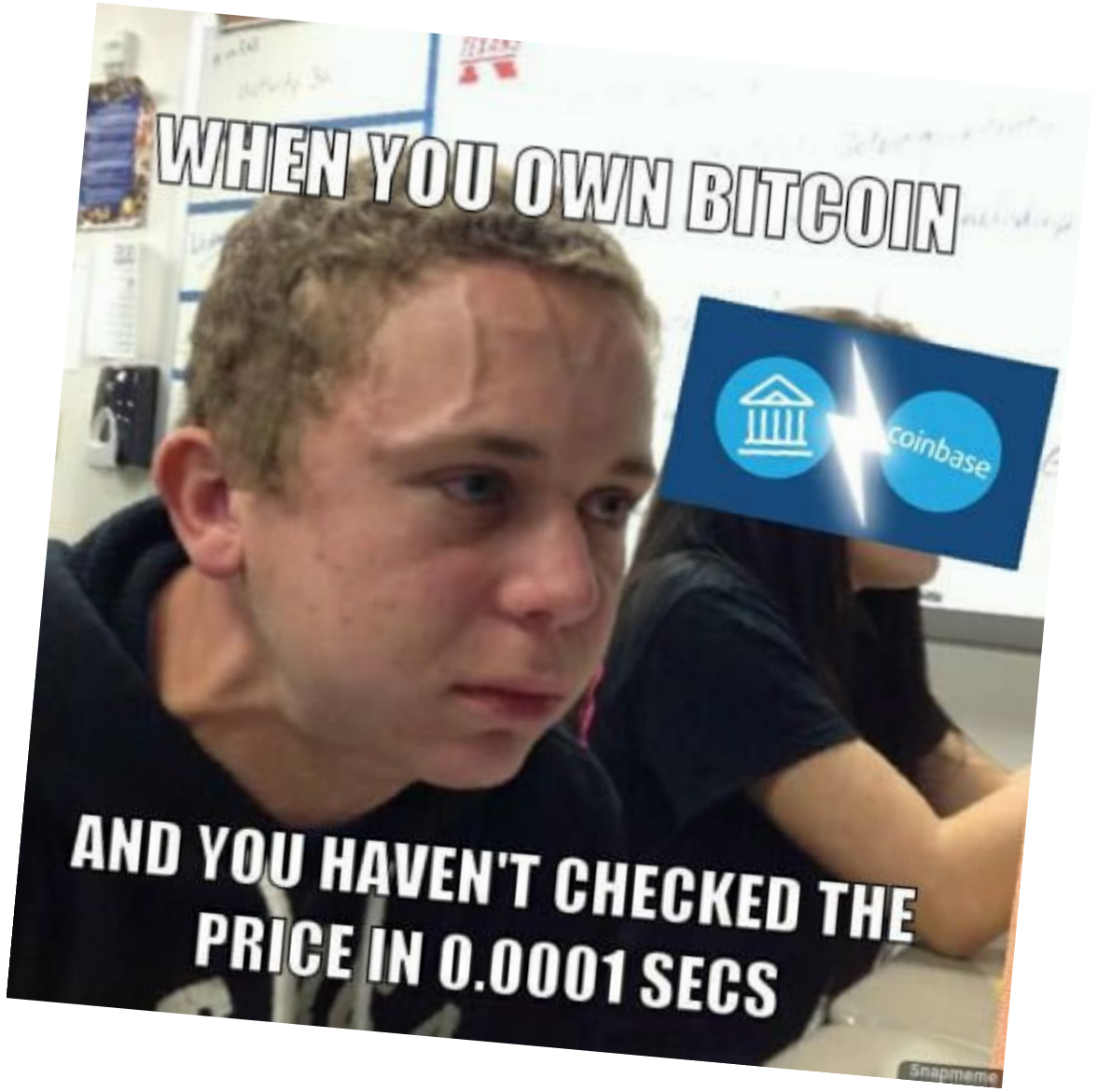
REWARDS	# TICKETS GIVEN	CONSEQUENCES	# TICKETS TAKEN AWAY
 Extra Math	+5	 HITTING	-3
 Getting along WELL with others	+3	 BULLYING	-4
 Good Table Manners	+4	 TEASING	-1
 LOVE & RESPECT	+5	 LYING	-2
 Obeying the FIRST TIME	+3	 THROWING A FIT	-3
 Calm & Quiet in STORE	+3	 Ignoring Parents	-4
 Extra Reading	+2	 SCREAMING or YELLING	-1
 CLEANING up after PLAYING	+2	 BAD SPORT	-2

Stability

- **Equilibrium Performance**

  Agents behave as intended (assuming everyone else does so)

  System performs in the desired way



Stability

- **Remain Decentralized**

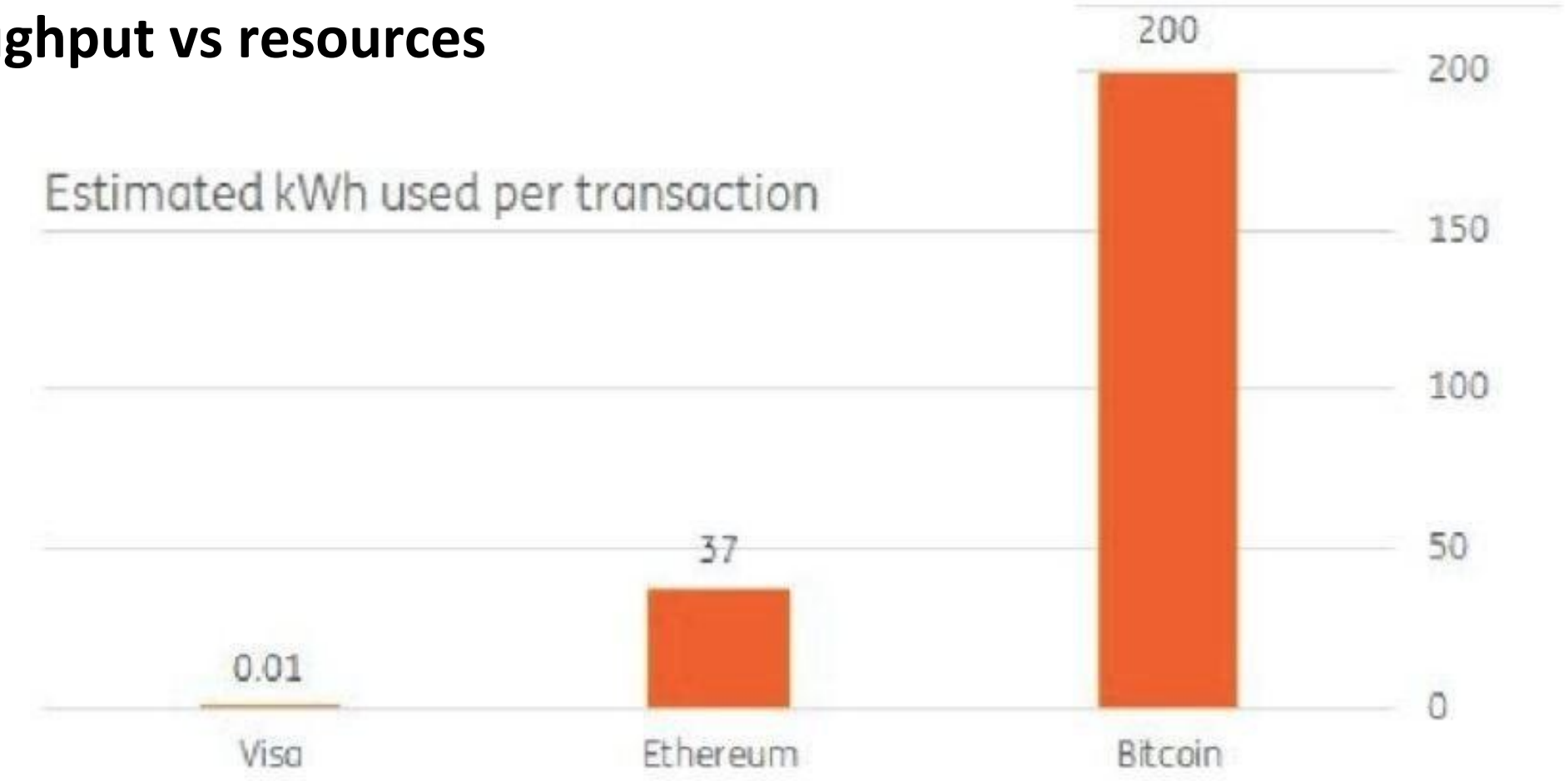
  System is sustained without a central authority that regulates “governs” the blockchain.

Efficiency

- **Does the protocol achieve its goals (output) at a low cost (input of resources)?**

Efficiency

- **Throughput vs resources**



Efficiency

- **Throughput vs resources**

Source: https://powercompare.co.uk/bitcoin/

Efficiency

- **Throughput vs resources**

Source: https://powercompare.co.uk/bitcoin/

Efficiency

- **Scalability:**
  - Handle more transactions (but not only)
  - Also: Increase performance as users increase

    (like BitTorent)

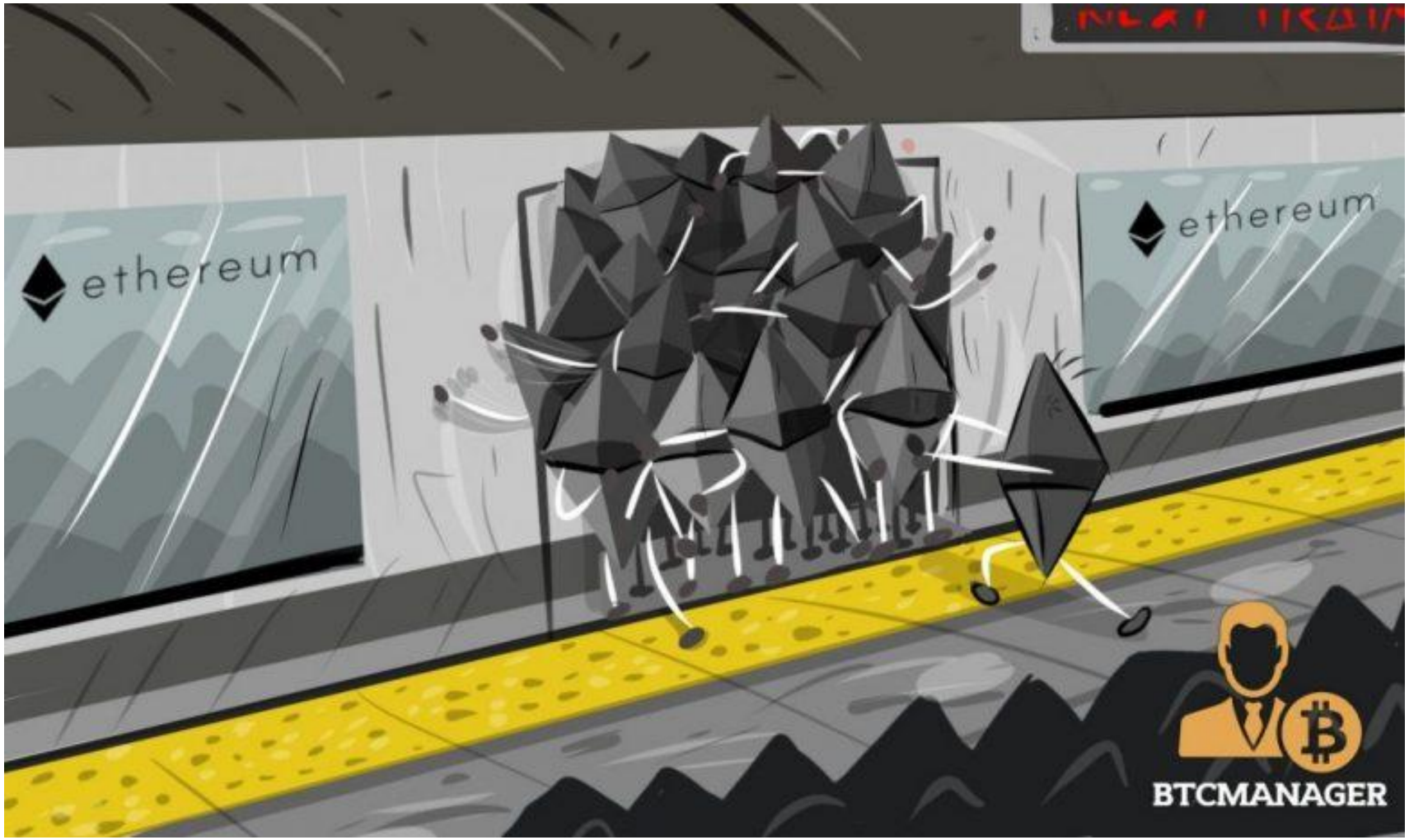
Efficiency

- **Scalability:**

  Imagine a train that

  - cannot take all passengers

  - is slower with more passengers



Efficiency

- **Scalability:**

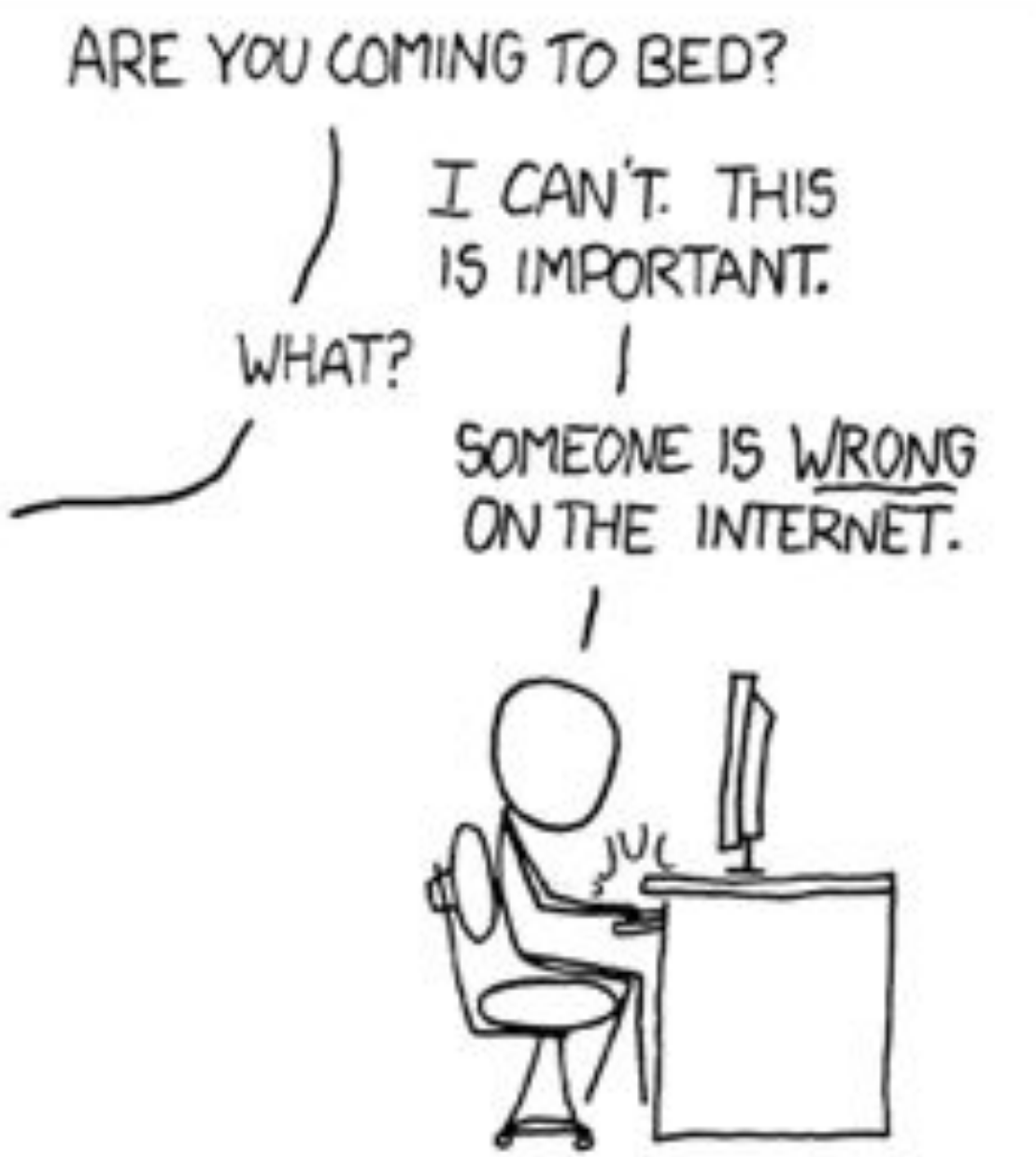
  We want exactly the opposite!

Efficiency

- **Latency**

  Processing and confirmation times of transactions must be fast.

  Latency may also refer to other properties...



Robustness

- **Most protocols** continue to operate optimally, i.e., deliver liveness and safety (consensus), even if some (minority) of the participants deviate.
- **Fault Tolerance:** 51% majority or 67% super-majority.

Robustness

- **How does the protocol cope with slight perturbations in its assumptions/behaviour of the participating agents?**
- **Or:** how do performance measures respond relative to deviations from equilibrium behaviour.
- **Keep in mind:** several measures that quantify performance hence robustness can be measured in many ways.
  - Equilibrium refinements: immune/resilient/coalition proof equilibria ...
  - Price of Anarchy (PoA)
  - (λ, μ) Robustness

Persistence

- **Can the protocol dynamically recover its equilibrium state if it starts from a totally different state?**
- **Or:** how does the protocol cope with large perturbations in its assumptions/behaviour of the participating agents**?**

Persistence

- **Recovery Mechanisms** from attacks
- **Non-equilibrium** dynamics:

  Starting from a totally perturbed state, can the protocol recover the desired equilibrium?
- **51% Attacks** - Forks etc.

Q&A?


I DON'T KNOW
HOW BITCOIN WORKS
AND AT THIS POINT
I'M TOO AFRAID TO ASK
imgflip.com

Proof-of-Stake: Propose blocks by temporarily locking tokens on the blockchain

Transition from PoW to PoS: Casper the Friendly Finality Gadget

How: Validators periodically vote on checkpoints on PoW chain

Uniqueness: **Checkpoints every 50 blocks**

Other POS protocols:

NXT, Blackcoin, Tezos, Ouroboros

Similar to POS protocols:

EOS, Tendermint, NEO, NEM, Algorand

Types of attacks/faults

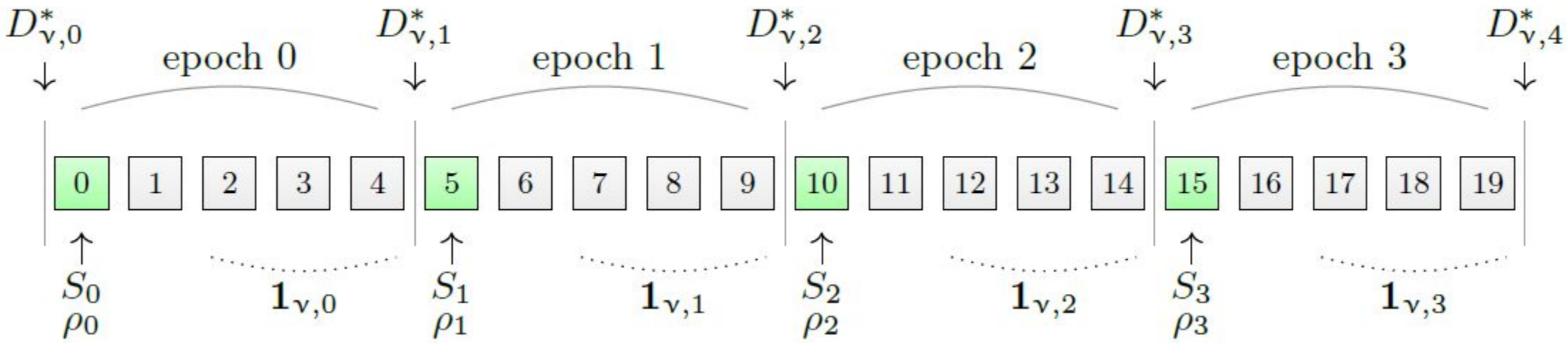
1. Validators voting for conflicting checkpoints (safety faults)
   - slashing
2. Invalid votes (liveness faults)
   - Not in time (latency)
   - Not cast
   - Not propagated
   - Voted for the ‘wrong’ block
   - ….

P.R.E.ST.O

- **Optimality**
  - PoW chain's optimality (eventual liveness and safety)
  - Ethereum Virtual Machine: smart contracts
  - Universal Turing Machine: compatible with "any" programming language
  - ...

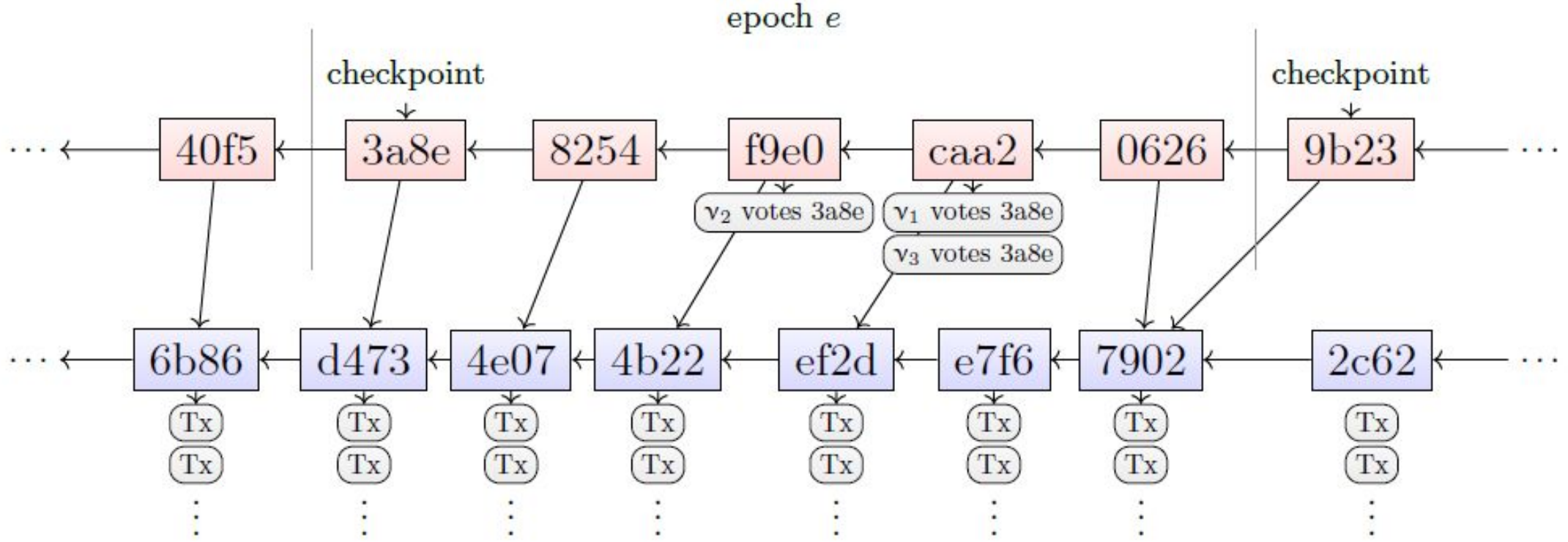
P.R.E.ST.O

- **Stability:** Enhanced by checkpointing mechanism



casper P.R.E.ST.O

- **Efficiency:** Dual Chain approach

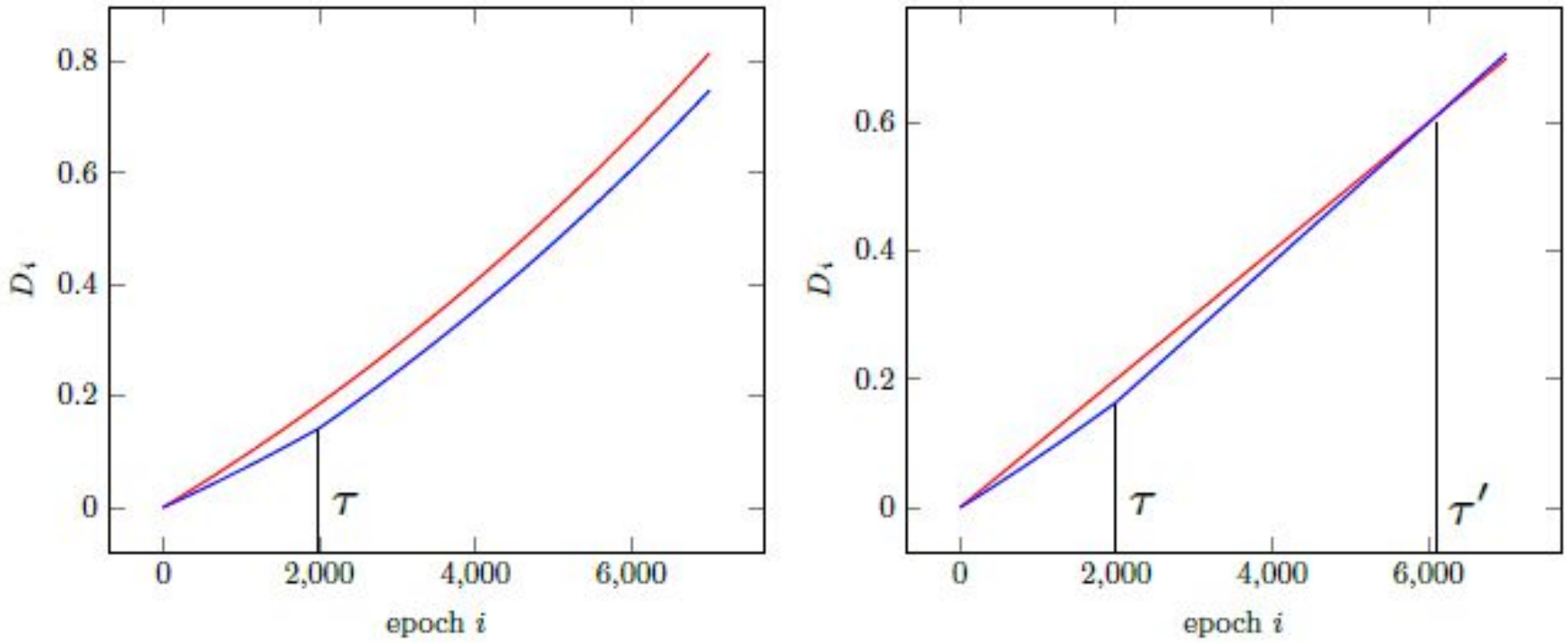


P.R.E.ST.O

- **Robustness:**
  - Two types of obvious attacks: abstaining and censoring
    - Both hurt *all* validators' deposits in the short-term
    - Furthermore, ratio of victims' damage to attackers' damage can often be upper-bounded
    - Censorship of other validators' votes: profitable only for certain protocol parametrization and for the very long-term

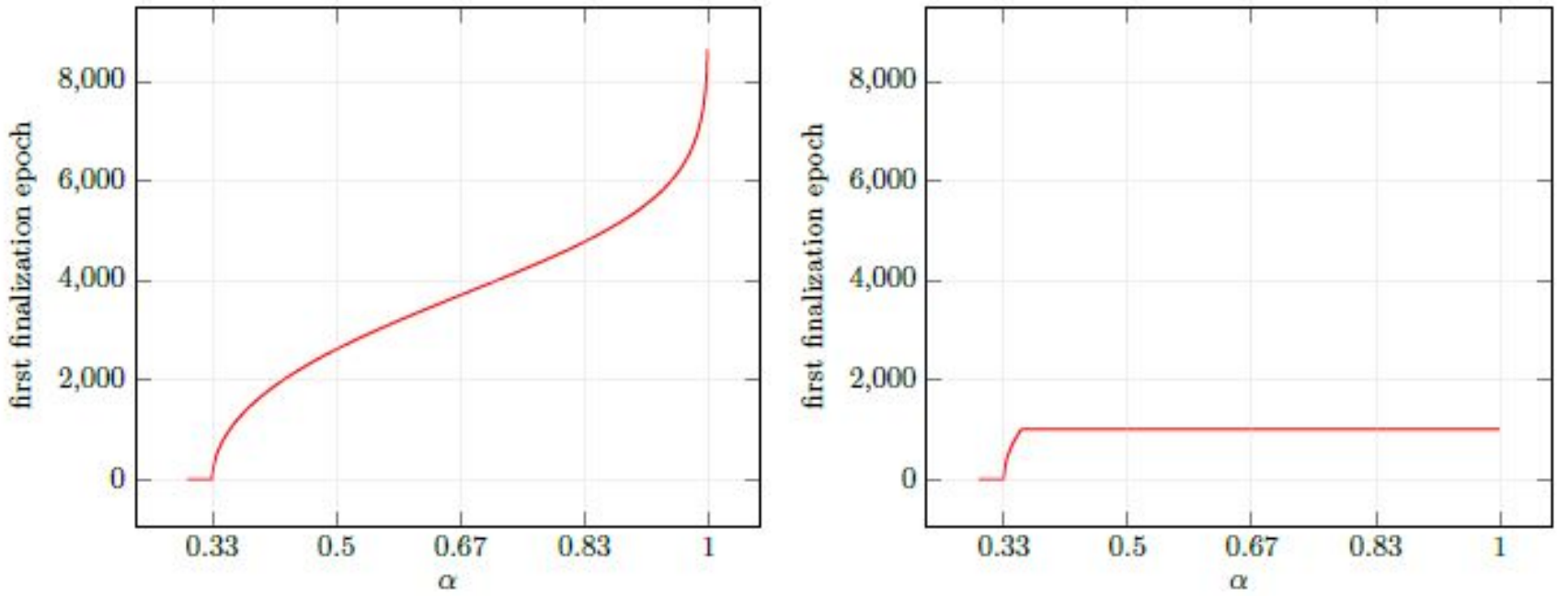
P.R.E.ST.O

- **Robustness:** Long-term guarantees



P.R.E.ST.O

- **Persistence:** Minority Forks -- Resuming Finality



(a) Benchmark setting. (b) Added exponential penalty term.

Q&A?


I DON'T KNOW
HOW BITCOIN WORKS
AND AT THIS POINT
I'M TOO AFRAID TO ASK
imgflip.com

Break

Blockchain in SUTD

Research interests:

- Georgios: incentives
- Sun Jun: formal verification
- Pawel: security

Activities:

- Cryptocurrency Clone Detection

Blockchain@NTU

- Student-led club
- Current club size: 40+ members
- Good variety of disciplines and experience
- Mentored by Prof Wen Yonggang and Prof Sourav

What We Do

BLOCKCHAIN AT NTU

- 3 Branches: Education, R&D, Consulting
- Main Focus for 2018: Education
- Fortnightly Lectures
  - Recorded and open to the public
- Workshops with external speakers
  - Ziliqa, Bluzelle, Bitmain, etc

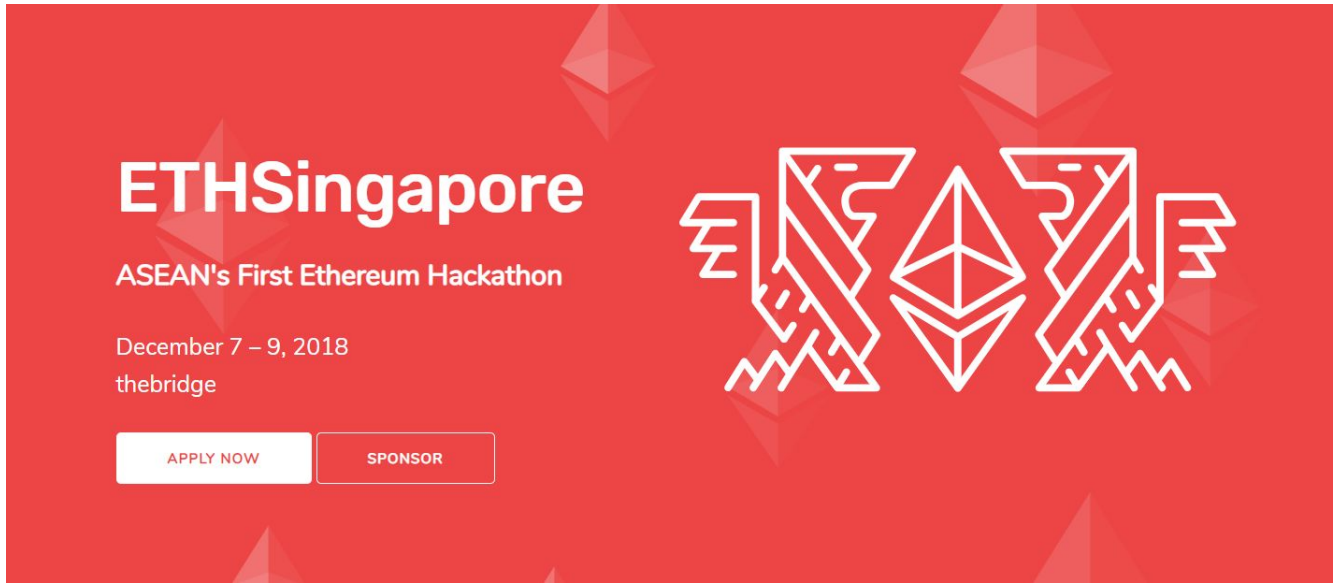
SWTRD

BLOCKCHAIN RESEARCH COLLECTIVE

Events & Outreach

BLOCKCHAIN AT NTU

- ETHSingapore
  - ethsingapore.co
- The Blockchain Campus



BLOCKCHAIN RESEARCH COLLECTIVE

Ongoing Research (Graduate)

BLOCKCHAIN AT NTU

Prof Wen Yonggang : Designing robust Blockchain Architecture and Protocols
Working closely with Vitalik, and on some Government projects with Liu Yang

Prof Kwok-Yan Lam : Security and Privacy enabled Blockchain Architecture
Project with Industry partners, in collaboration with NRF, on Supply Chain

Prof Ng Wee Keong : Highly Scalable Enterprise Blockchain Applications
Project RealChainDB based on Apache Cassandra, various industry projects

Prof Liu Yang : Security of Smart Contracts and Core Blockchain Designs
Projects with Government, some PhD students, discovered many vulnerabilities

Prof Dusit Niyato : Applications of Blockchain in Energy Sector
Working on Government projects, with the Industry, has some PhD students

Prof Anupam Chattopadhyay : Merger of Blockchain with IoT and CPS
Working on Supply Chain projects with Prof Lam, looking at Hardware solutions

Prof Anwitaman Datta : Blockchain Protocols and Distributed Systems
Working on core Blockchain protocols and incentive design, teaching courses

Dr Sourav Sen Gupta : Secure and Privacy-preserving Blockchain Solutions
Working on privacy preservation and security, designing and teaching courses

Dr Zhao Jun : Security and Privacy issues in Enterprise Blockchain Solutions
Working closely with Prof Niyato on some industry projects in Energy sector

SWTR

BLOCKCHAIN RESEARCH COLLECTIVE

Activities

- SCILLA workshop in conjunction with opening of CRYSTAL Center on 12th November
- Github Organisation

Collaborative space for research on technical aspects of blockchain