BLOCKCHAIN INCENTIVES: CRYPTOECONOMICS AND PROOF-OF-STAKE

Gillian Chu
Brian Ho

LECTURE OVERVIEW

1. CRYPTOECONOMICS
2. CRYPTOGRAPHY
3. ECONOMICS
4. PROOF-OF-STAKE
5. ATTACKS

1 CRYPTO ECONOMICS

WHAT IS CRYPTOECONOMICS?

BLOCKCHAIN FUNDAMENTALS

CRYPTOGRAPHY

ECONOMICS

PRESENT

PAST

FUTURE

WHAT IS CRYPTOECONOMICS?

BLOCKCHAIN FUNDAMENTALS

CRYPTOGRAPHY

PAST

PRESENT

ECONOMICS

FUTURE

WHAT IS CRYPTOECONOMICS?

BLOCKCHAIN FUNDAMENTALS

CRYPTOGRAPHY

PAST

PRESENT

ECONOMICS

FUTURE

DISCUSSION

BITCOIN'S DESIRED PROPERTIES

BLOCKCHAIN FUNDAMENTALS

Immutable

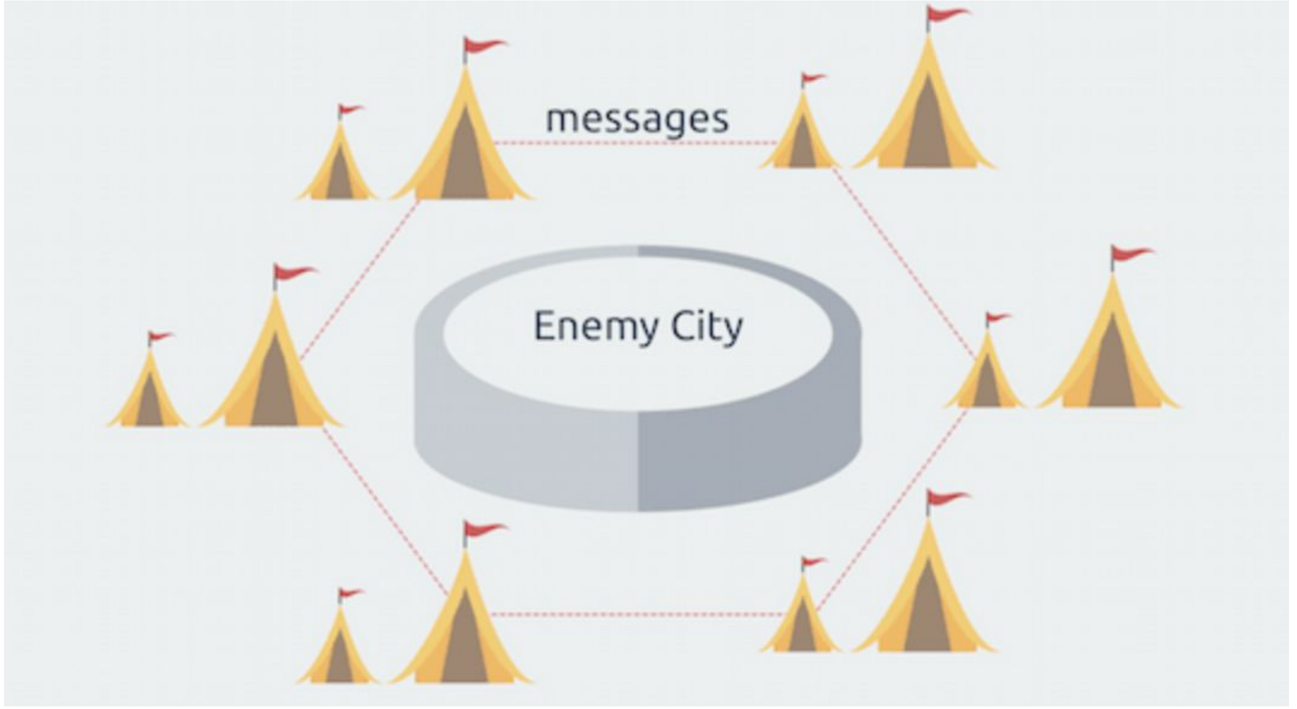
Valid()

Tx $$

Accessible

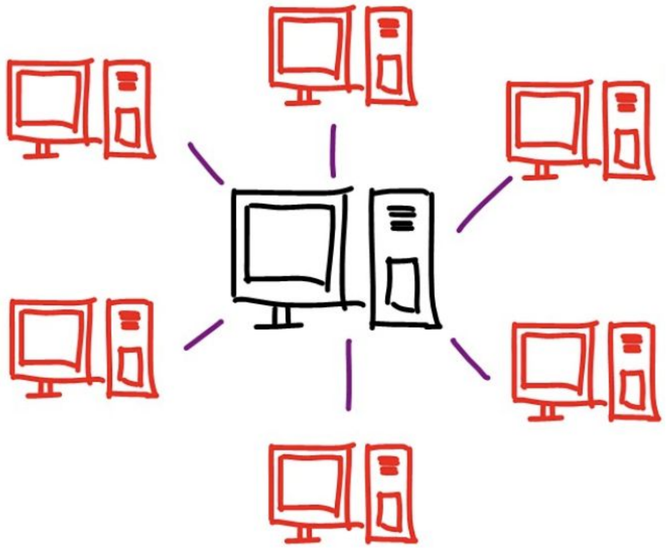
BYZANTINE GENERAL'S PROBLEM

BLOCKCHAIN FUNDAMENTALS



BYZANTINE FAULT TOLERANCE

THE PROBLEM WE'VE REALLY BEEN DEALING WITH



	The Situation	
Agree on a Strategy	Objective	Agree on Valid Transactions
Separated Camps	Spacial Distribution	Distributed Nodes in the Network
Loyal Troop and Loyal Generals	The Good Ones	Truthful Nodes
Traitors	The Bad Ones	Evil Nodes
Corrupt a Message	The Attack	Add an Invalid Transaction to the Blockchain
How to Know which Message is True	The Problem	How to know which Transaction is Valid
Don't Have	A Solution	Proof of Work
Don't Have	Consensus	Blockchain with More Combined Difficulty

2 CRYPTOGRAPHY

USES OF CRYPTOGRAPHY

HASHES

Prove immutability of the blockchain, i.e topological sorting of blocks

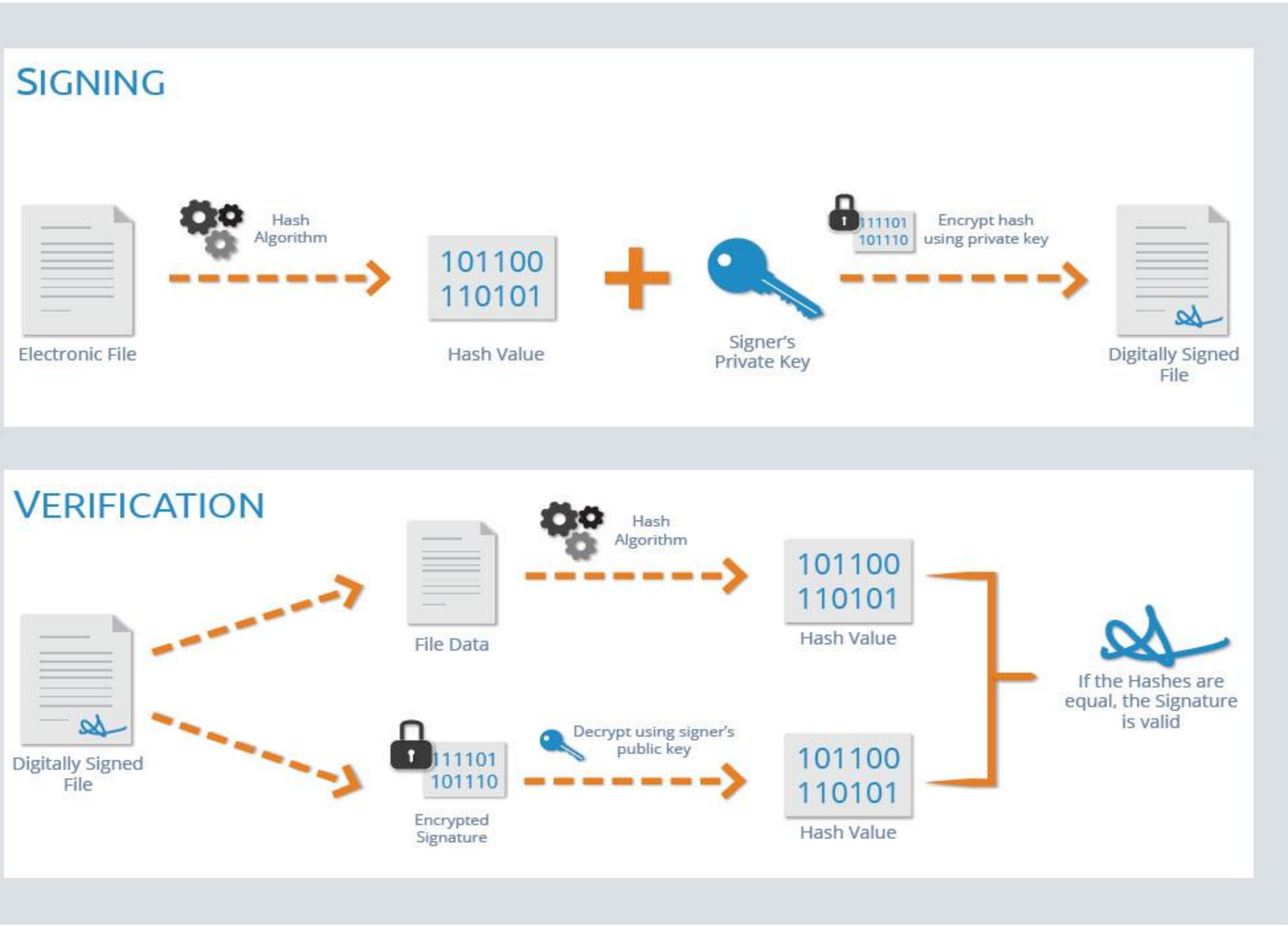
=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

USES OF CRYPTOGRAPHY

SIGNATURES

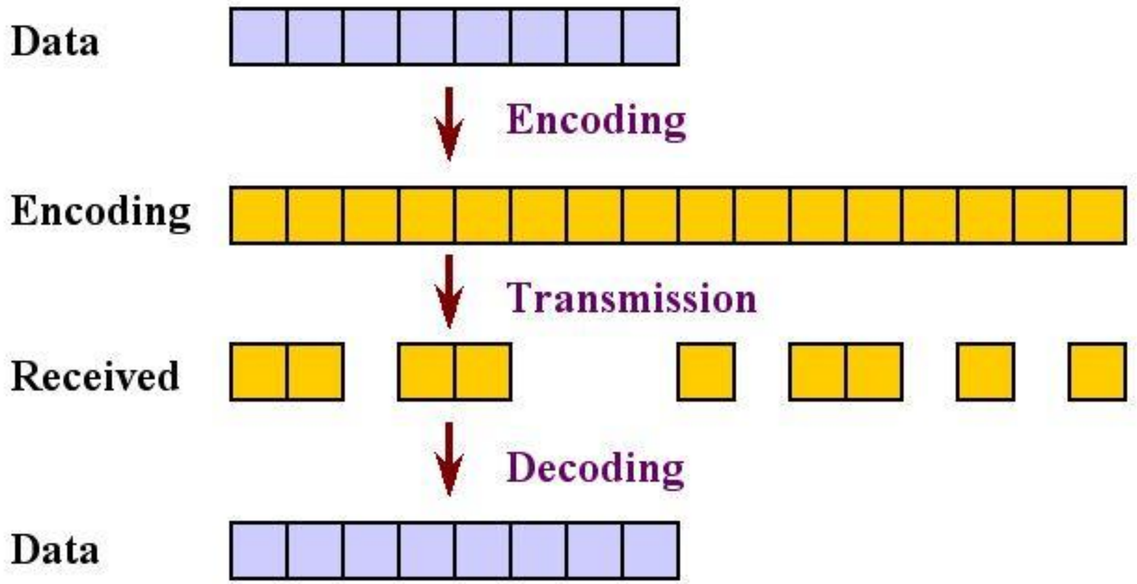
Help verify identity of the sender



USES OF CRYPTOGRAPHY

ERASURE CODES

Lowers the 100% data availability requirement



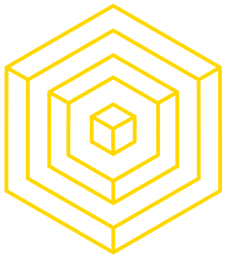
USES OF CRYPTOGRAPHY

TIMELOCKS

Prove **some time has elapsed** between messages A and B

- Flavor of encryption which takes some time to decrypt
- Parallelization Speed-up is Useless

$$d = c^{2^n} \mod pq$$



SUMMARY SLIDE

FORMALIZING A NEW PERSPECTIVE

Erasure Codes	Immune to data unavailability attacks
Hashes	Provide topological ordering of messages
TimeLock (Sequential PoW)	Prove time elapse between messages
Signatures	Prove identity of sender of message

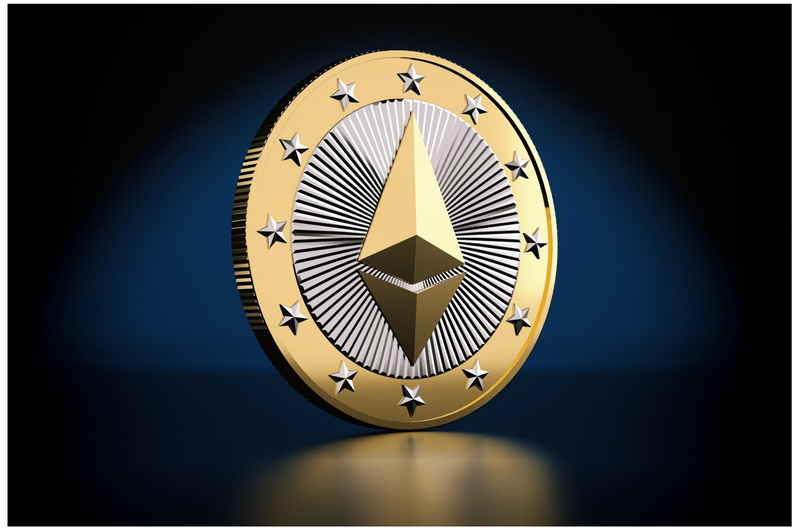
3 ECONOMICS

3.1 GAME THEORY

ECONOMIC INCENTIVES

REWARDS AND PENALTIES

- **Tokens:** Units of a protocol-defined cryptocurrency given out to miners. Eg: **block rewards**.
- **Privileges**: Decision making rights they can charge for. Eg. **transaction fees.**



ECONOMIC INCENTIVES

REWARDS AND PENALTIES

DISCUSSION

ECONOMIC INCENTIVES

CONCEPTS

SECURITY MARGIN

ECONOMIC INCENTIVES

CHOICE MODELS

Uncoordinated choice model:

- Assumes participants do not coordinate with each other
- Have separate incentives, ALL SMALLER than security margin X

ECONOMIC INCENTIVES

CHOICE MODELS: ROUSSEAU

	Cooperate	Defect
Cooperate	3 3	2 0
Defect	0 2	1 1

ECONOMIC INCENTIVES

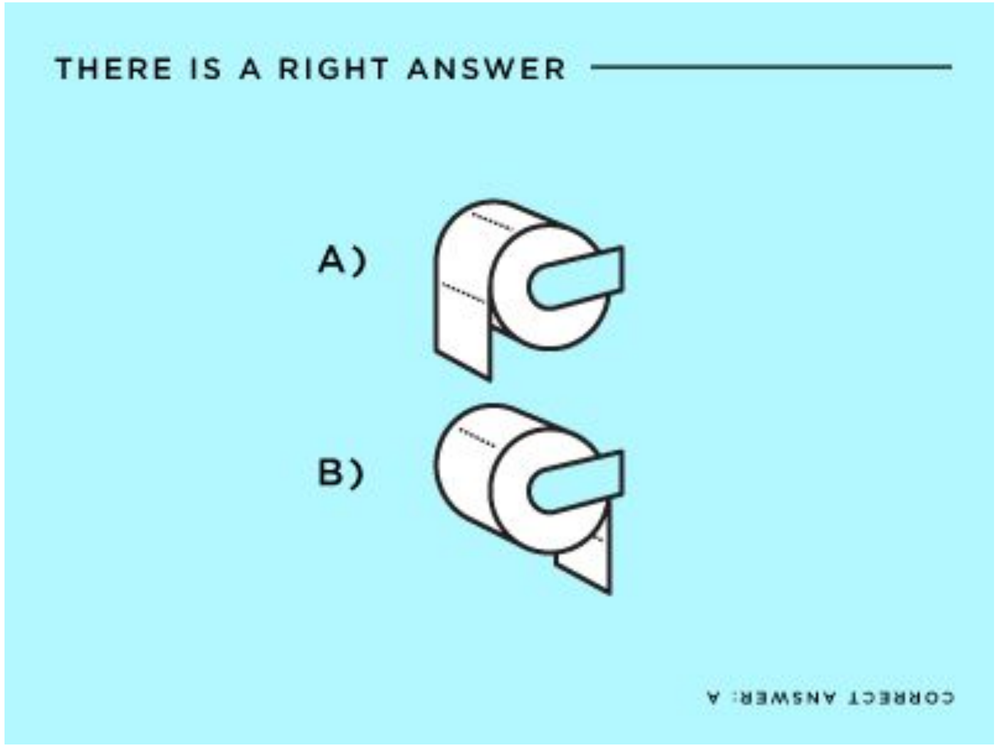
CHOICE MODELS: DATE NIGHT

Coordinated choice model: A model that assumes that all actors in a protocol are controlled by the same agent (or coalition).

MAN \ WOMAN	Boxing	Shopping
Boxing	2 , 1	0 , 0
Shopping	0 , 0	1 , 2

VITALIK'S SCHELLINGCOIN

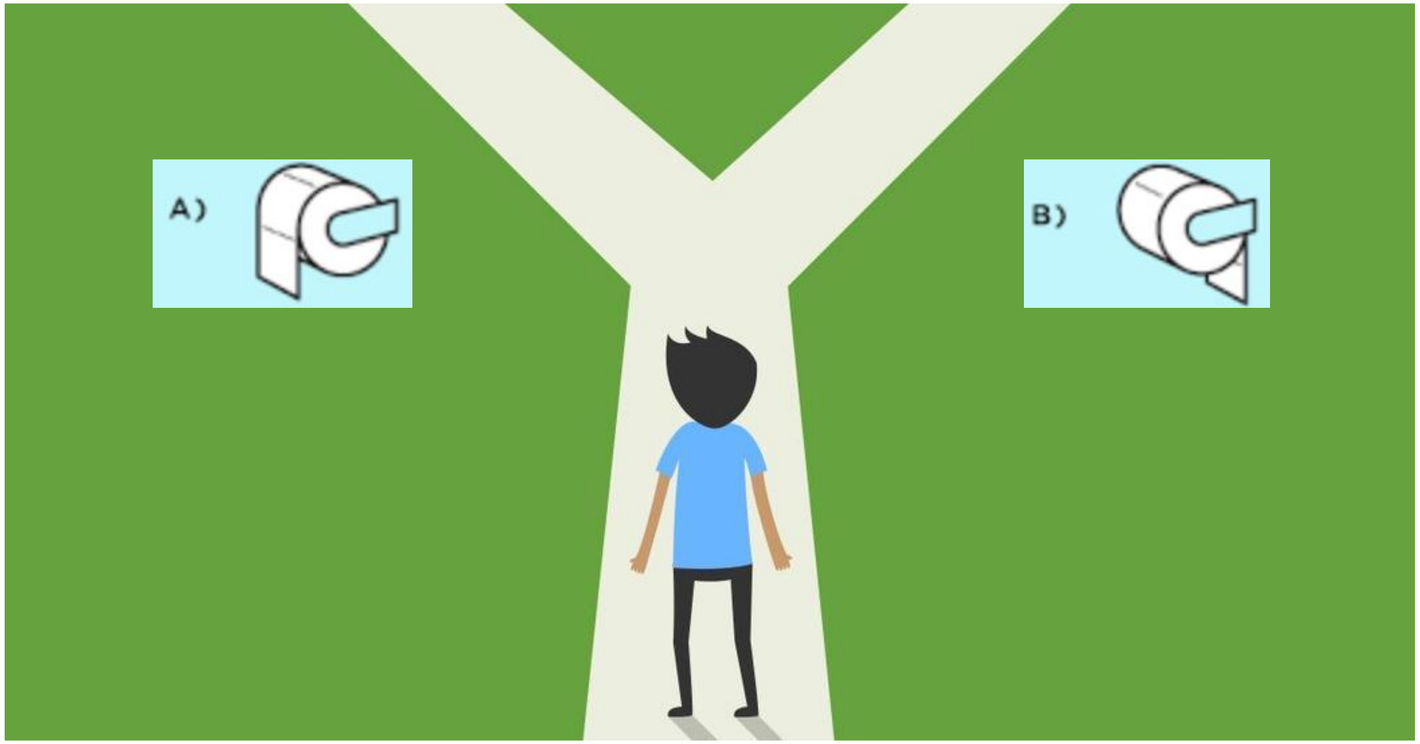
AN EXPLANATION



VITALIK'S SCHELLINGCOIN

AN EXPLANATION

Provide the "true answer" to:



QUESTIONS?

ECONOMIC INCENTIVES

CHOICE MODELS: BRIBING ATTACK MODEL

Economically rational people need to vote the “truth” or at least what they think majority will vote.

Uncoordinated Game

	You Vote A	You Vote B
Others Vote A	P	0
Others Vote B	0	P

Bribing Attacker Game

	You Vote A	You Vote B
Others Vote A	P	P + ε
Others Vote B	0	P

ECONOMIC INCENTIVES

CHOICE MODELS: BRIBING ATTACK MODEL

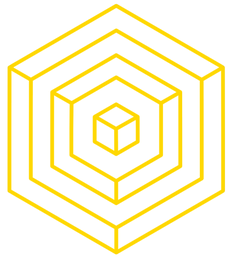
Economically rational people need to vote the “truth” or at least what they think majority will vote.

Uncoordinated Game

		ote B
Others Vote A		
Others Vote B		

Bribing Attacker Game

	You Vote A	You Vote B
Others Vote A	P	P + ε
Others Vote B	0	P



3.2 ATTACKS

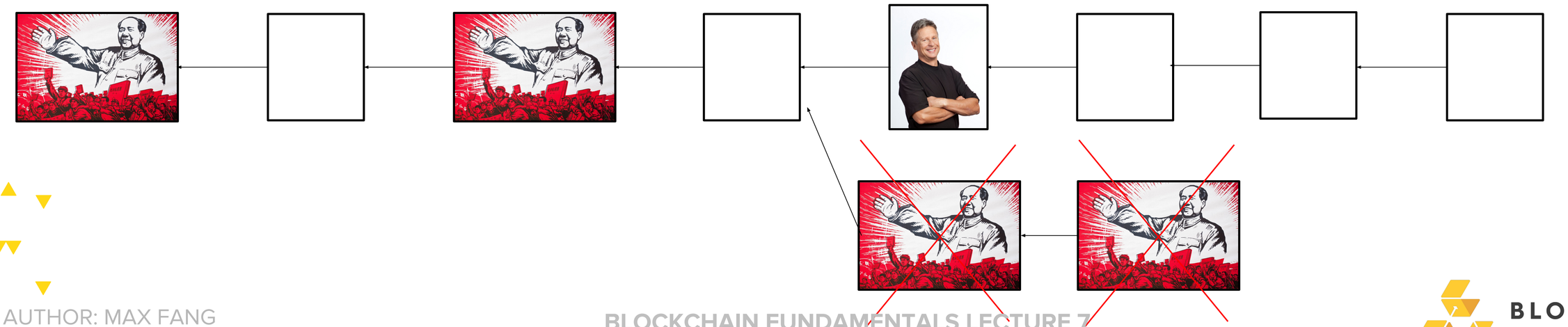
REVIEW: ATTACKS

FEATHER FORKING

Announce that you will **attempt** to fork if you see a block from Gary, but you will give up after a while

- As opposed to attempting to fork forever; doesn't work without >51%

- Ex. Give up after block with Gary's tx contains **k** confirmations



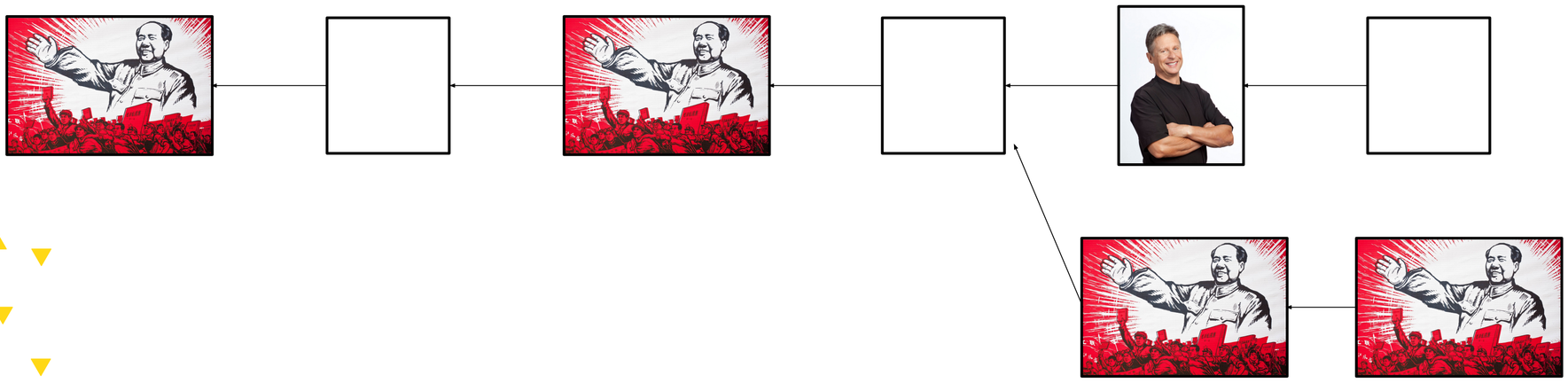
REVIEW: ATTACKS

FEATHER FORKING

Let **q** equal the proportion of mining power you have, 0 < **q** < 1
Let **k** = 1: You will give up after 1 confirmation (one additional block)

- Chance of successfully orphaning (invalidating) the Johnson block = $\mathbf{q^2}$

If **q** = **.2**, then $\mathbf{q^2}$ = **4%** chance of orphaning block. Not very good

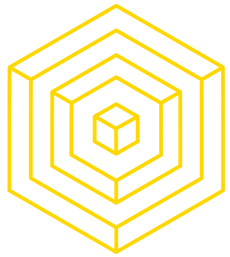


BLACKLISTING

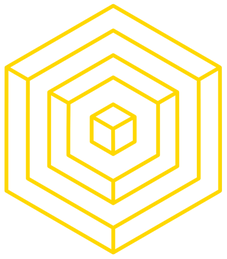
FEATHER FORKING

	You Include	You Don't Include
Block Accepted	$(1-q^2)$ * Blockreward + Johnson's tx fee	BlockReward
Block Rejected	0	0


BREAK
SECTION
BLOCKCHAIN
AT BERKELEY



4 PROOF OF STAKE



PROOF-OF-WORK

DRAWBACKS

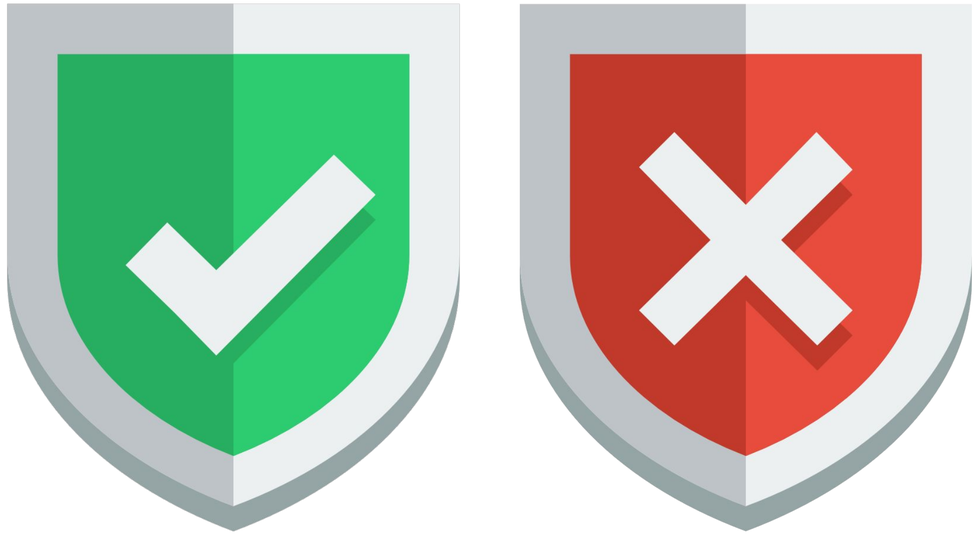
"What are some drawbacks of Proof-of-Work?"

PROOF-OF-WORK

DRAWBACKS

In Proof-of-Work, there's no defender's advantage:

- The cost of attack and the cost of defense are 1:1 ratio
- Constraints are inflexible (i.e. computation, electricity)



There is nothing in place to *prevent* or *discourage* malicious actors. Proof-of-Work simply allows it.

PROOF-OF-STAKE

MOTIVATIONS

In Proof-of-Stake, you can specify properties you want to maintain a "defender's advantage"

- Introduce penalties
- Punish malicious behavior much more greatly than in PoW
- Security comes from putting up economic value-at-loss

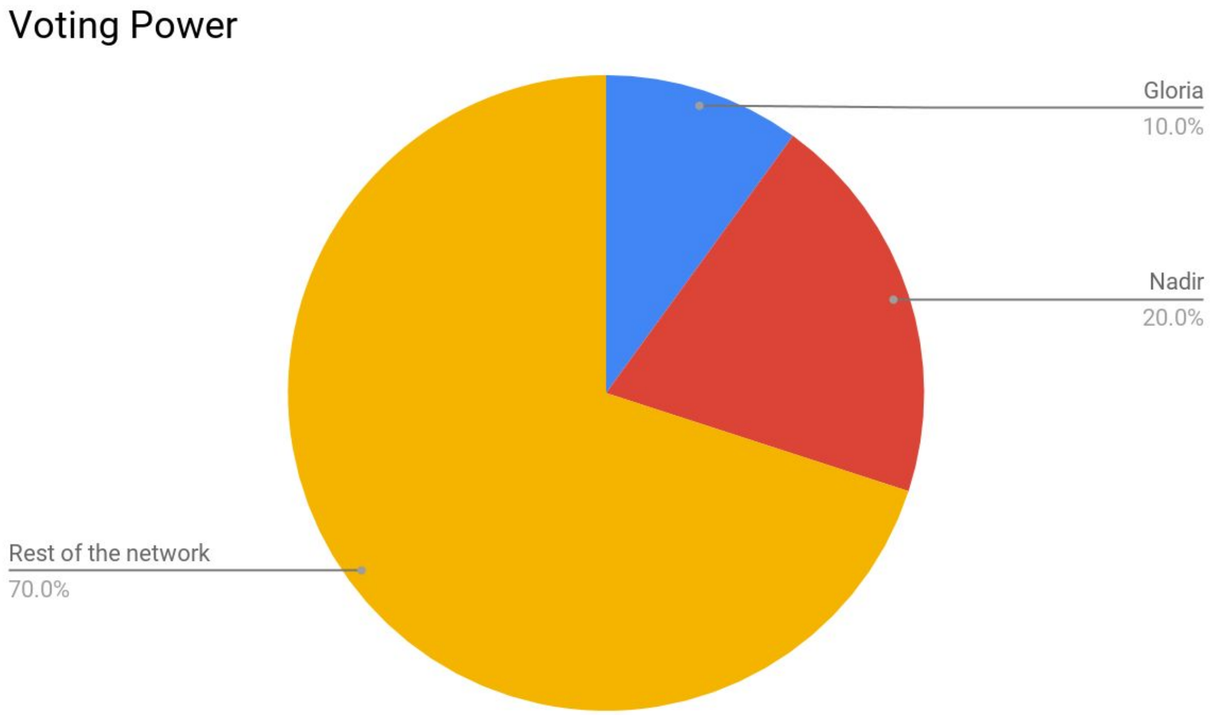
Discourage malicious behavior with explicit consequences

PROOF-OF-STAKE

WHAT IS PROOF-OF-STAKE?

Alternative Consensus algorithm where voting power is directly proportional to economic stake locked up in the network.

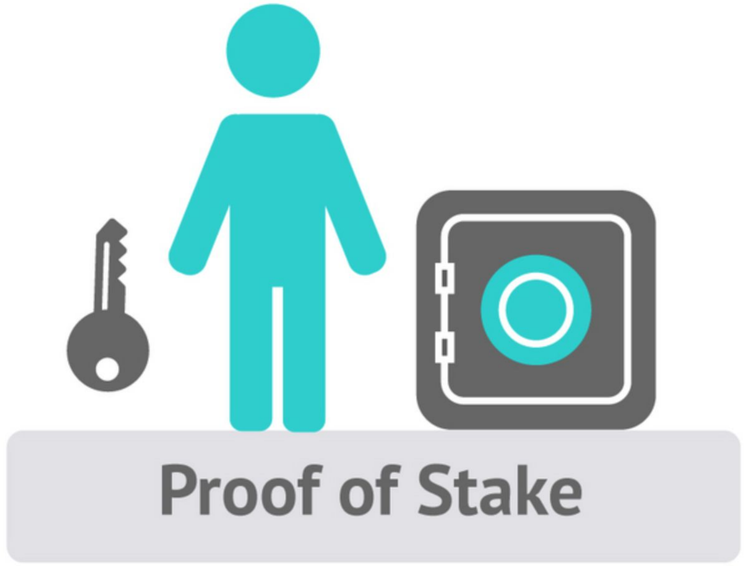
Examples: Casper (Ethereum), Tendermint, NXT, Peercoin, Blackcoin



POW VS POS?

DIFFERENCES

Miners have voting power proportional to the total computational power of the network.



Validators are stakeholders with voting power proportional to economic stake locked up.

POW VS POS?

DIFFERENCES

Proof of Work

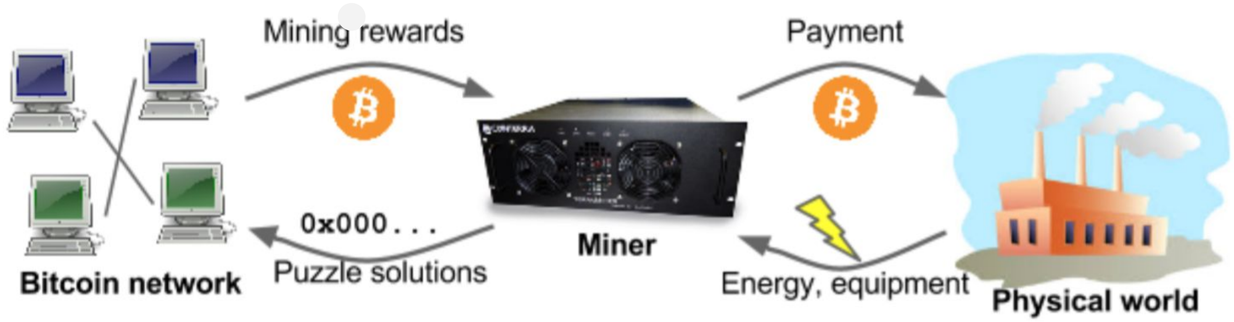


Figure 8.5: The cycle of Bitcoin mining

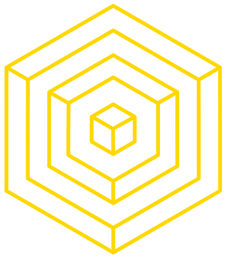
- 51% Attacks not disincentivized
- Rewards increase exponentially as you invest more money to buy hardware
- Unfair hardware distribution can cause centralization

Proof of Stake

Figure 8.6: The virtual mining cycle

- 51% Attack is like burning down your ASIC farm
- Rewards are directly proportional to stake in the system
- Hardware distribution cannot impact centralization
- More energy efficient

QUESTIONS?

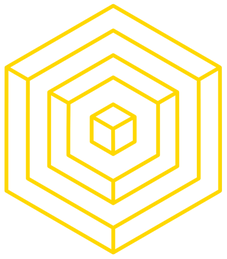


FLAVORS OF PROOF-OF-STAKE

MY CHAIN-BASED POS

Algorithm for Chain-based PoS:

1. Randomly choose a validator based on the proportional stake invested from the group of already existing validators.
2. The chosen validator *creates* a block which points to some previously created block.
3. The chosen validator gets the block reward and the transaction fees

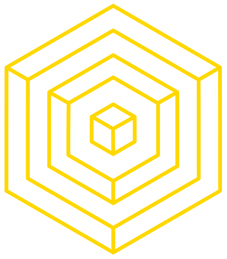


FLAVORS OF PROOF-OF-STAKE

MY BFT BASED POS

Algorithm for Byzantine Fault Tolerant PoS:

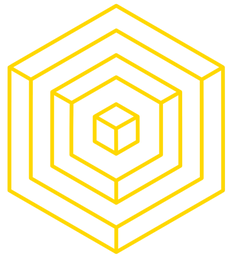
1. Randomly choose a validator based on the proportional stake invested from the group of already existing validators.
2. The chosen validator *proposes* a block
3. All the other validators vote yes if they think it is a valid block
4. If ⅔ or more voting power votes yes, the block is included in the blockchain. Otherwise a new proposer is chosen and we go back to Step 1.
5. The chosen validator gets the block reward and the transaction fees



PROOF-OF-STAKE

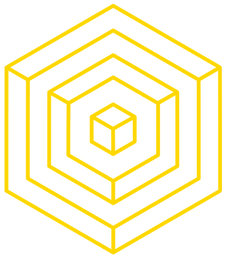
DRAWBACKS

- Rich get Richer
  - Richest participants given easiest mining puzzles in pure proof-of-stake
  - Dislodging 51% power is impossible
- Liquidity problem as funds are locked up
- Low participation can cause centralization
  - ASICS can be bought but stake cannot be accumulated unless a stakeholder sells
- Can rewrite history of blockchain if someone with a huge share of stake sells private keys



5

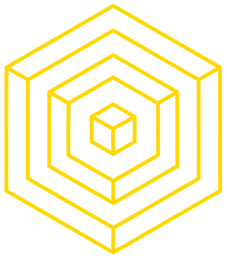
ATTACKS



NOTHING AT STAKE

EXAMPLE

"T/F: It is going to rain today."



NOTHING AT STAKE

EXAMPLE

"T/F: It is going to rain today."

my answers

correct answers		T	F
	T	1	0
	F	0	1

NOTHING AT STAKE

EXAMPLE

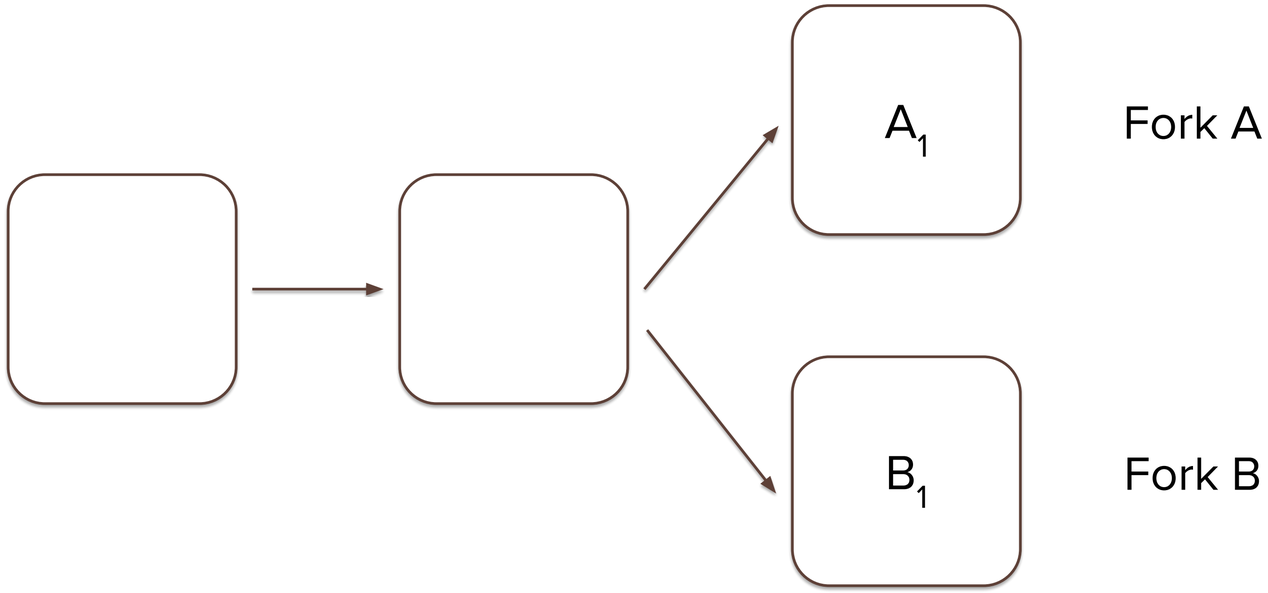
"T/F: It is going to rain today."

my answers

correct answers	T	F	none	**both**
T	1	0	0	**1**
F	0	1	0	**1**

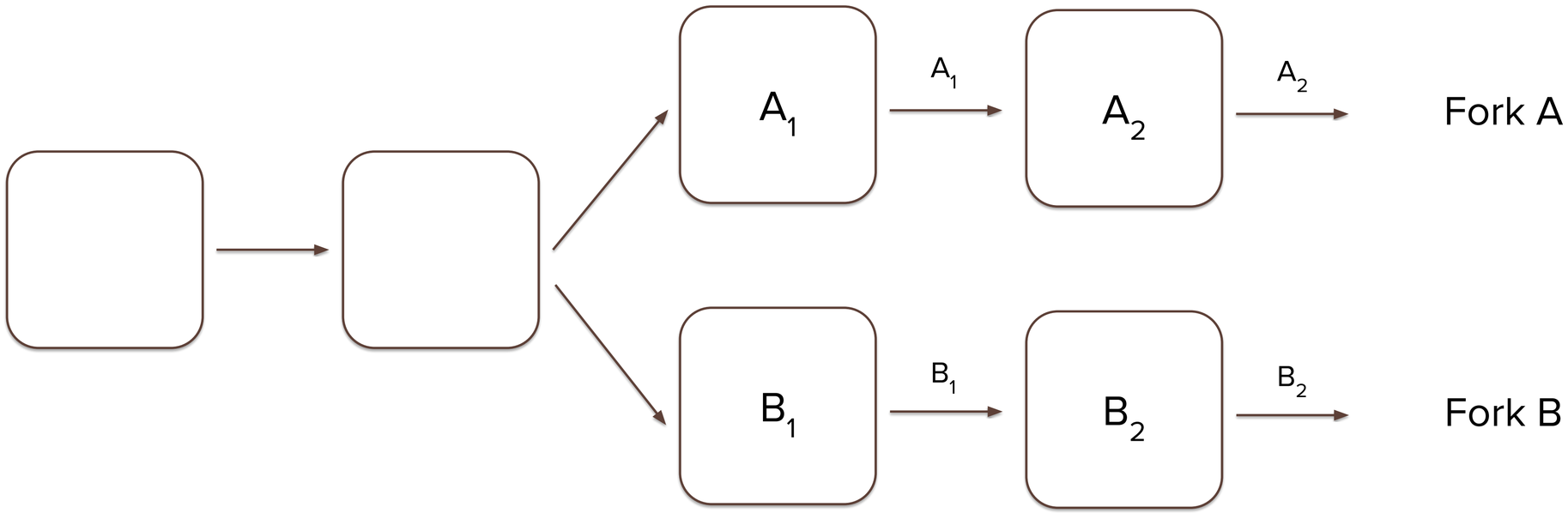
NOTHING AT STAKE

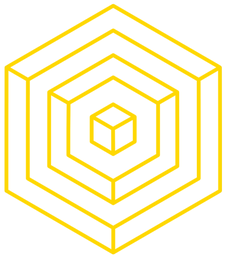
ATTACK



NOTHING AT STAKE

ATTACK





NOTHING AT STAKE

ATTACK

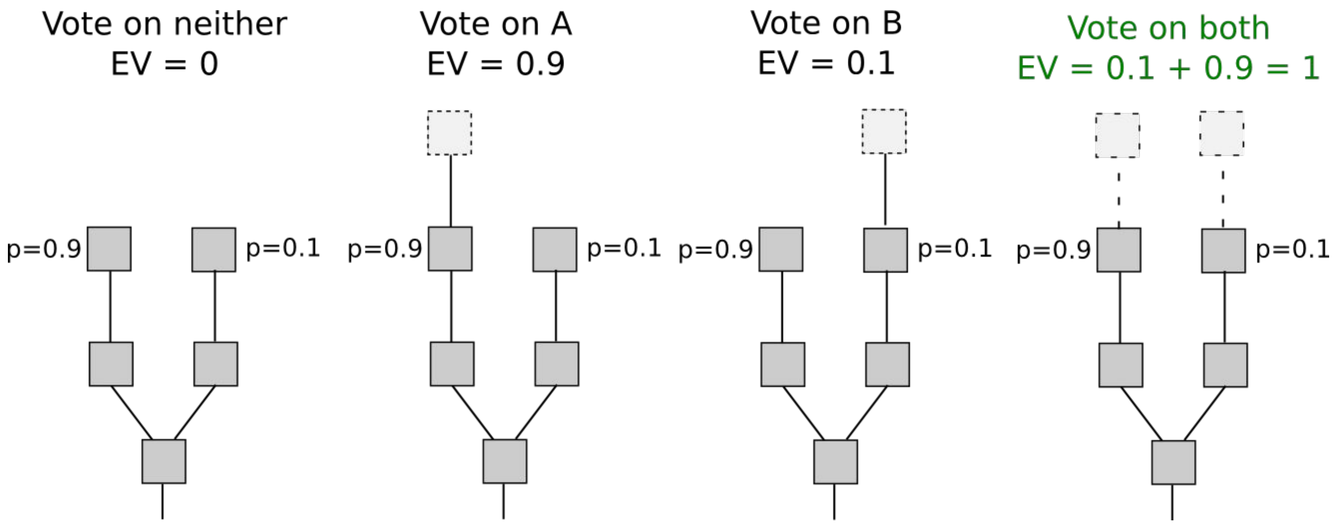
In chain-based Proof-of-Stake, validators know that if they create blocks on multiple competing chains they'll maximize their chances of getting a reward

- If actors are all economically rational, the blockchain never converges which means that the network never reaches consensus.
- Trade off between centralization and decentralized economically rational actors.

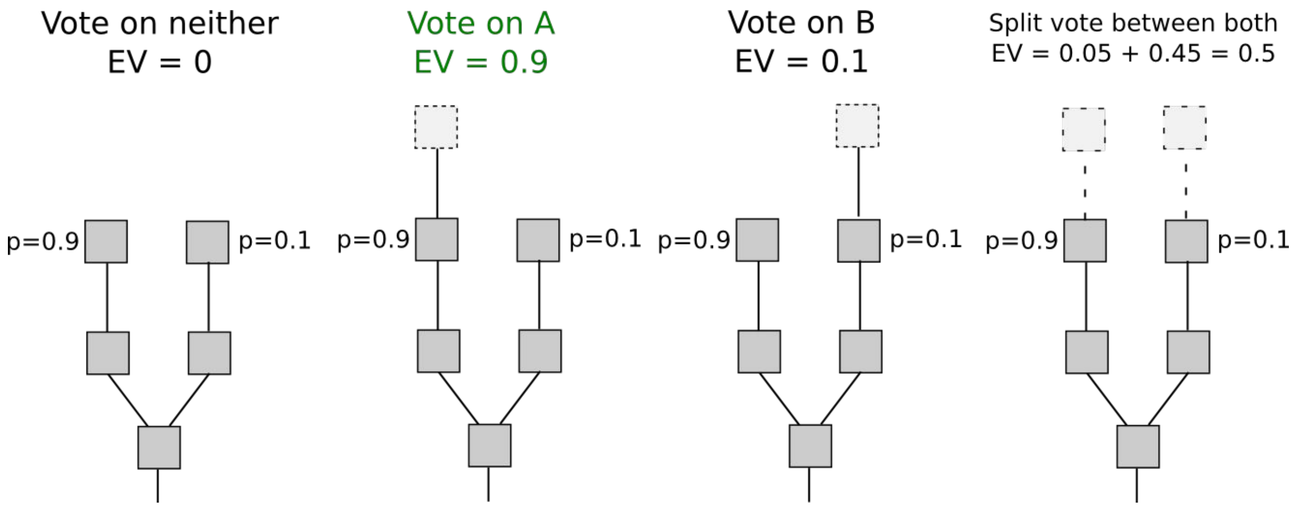
NOTHING AT STAKE

ATTACK

Naive Proof of Stake



Proof of Work



AUTHOR: BRIAN HO

NOTHING AT STAKE

DEFENSE

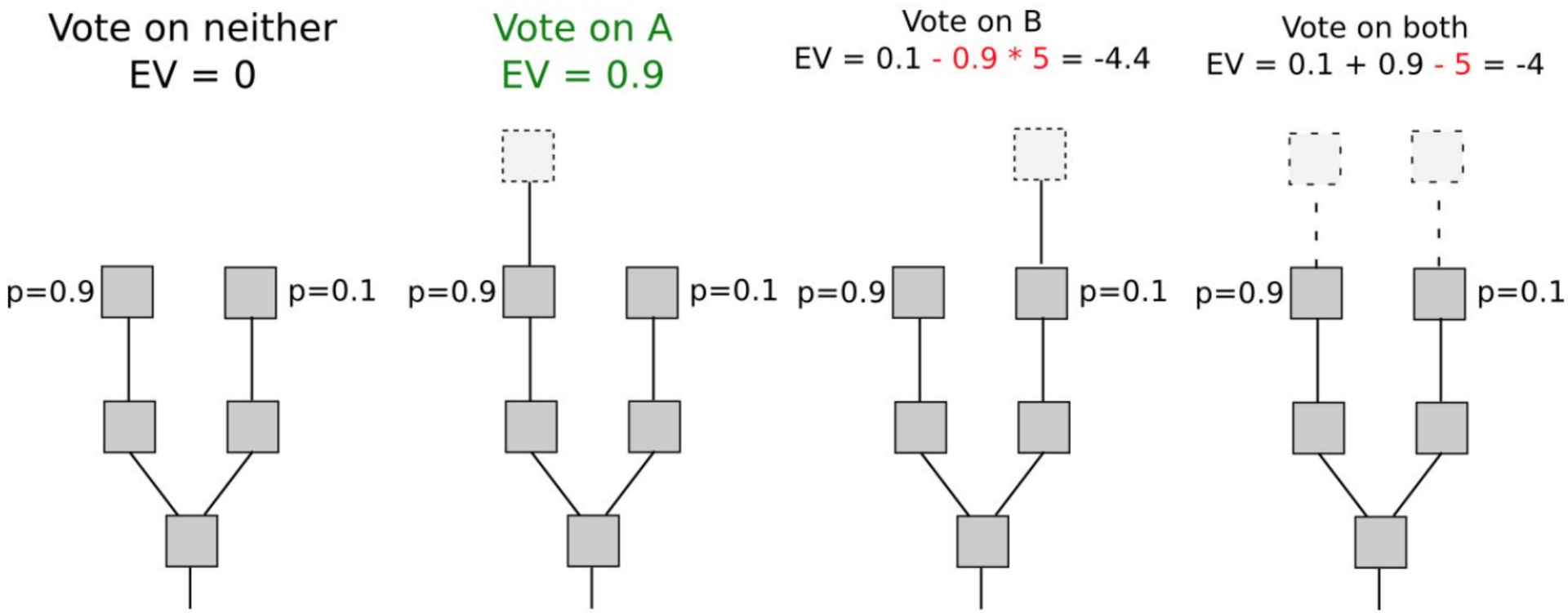
Slashing

- Make a rule that says: You are only allowed to “vote” on one fork
- Two possibilities:
  - If you are caught voting on the *wrong fork*, you get punished
  - If you are caught voting on *multiple forks*, you get punished

Rather than only having rewards, introduce penalties

NOTHING AT STAKE

DEFENSE



NOTHING AT STAKE

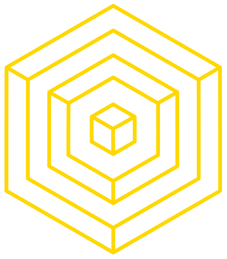
EXAMPLE

"T/F: It is going to rain today."

my answers

correct answers	T	F	none	**both**
T	1	**-1**	0	**-1**
F	**-1**	1	0	**-1**

QUESTIONS?



LONG RANGE ATTACK

ATTACK

Flawed Preconception:

“The longest chain is the most trustworthy and therefore the correct one”

In PoW, this is acceptable since the longest chain has the most *work* (time extensive operation) done on it which makes it *provably correct*

In PoS, there is no mining or any aspect of *work*

LONG RANGE ATTACK

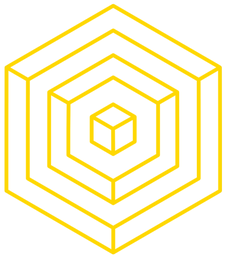
EXAMPLE

Suppose:

Gillian owns 1% of the tokens immediately after the genesis block is created.

- Starts “mining” on her own secret chain
- Since creating blocks doesn’t require any work, Gillian is able to easily create a longer chain that the current existing one
- If this new chain gets accepted as the “truth,” Gillian has successfully overwritten the entire blockchain history
- Long Range refers to the fact that this attack can start from any point in time (i.e. 1 block back vs 60,000 blocks back)

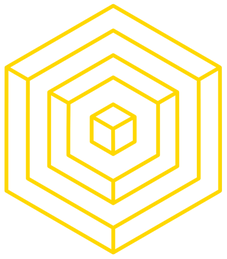
QUESTIONS?



STAKE GRINDING

ATTACK

- Problem: In a Proof-of-Stake ecosystem, need a way to randomly pick the next validator.
  - Need to pick an infinite sequence of validators in case the picked validator is offline
- Next chosen validator depends on previous block's signature.
  - The current validator can produce new signatures to improve his chance of being picked again.
  - In NXT, passing up the opportunity of being the validator for the current round gives the user a chance to manipulate randomness for future rounds

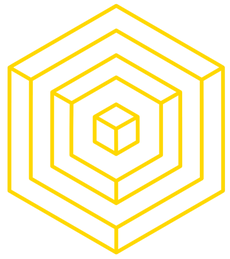


STAKE GRINDING

DEFENSE

- Don’t use any mutable parameters of the previous block as entropy to generate randomness
- Have all the validators deposit their stake well in advance.
- Have some sort of secret sharing/threshold signature scheme, through which multiple validators collaboratively generate the random value.
  - Unless majority colludes, this is a safe scheme

QUESTIONS?



READINGS

- Short overview of alternatives to PoW: https://www.coindesk.com/short-guide-blockchain-consensus-protocols/
- Stellar Consensus Protocol Overview: https://medium.com/a-stellar-journey/on-worldwide-consensus-359e9eb3e949
- CAP Theorem Overview: https://www.youtube.com/watch?v=Jw1iFr4v58M
- Raft Overview: http://container-solutions.com/raft-explained-part-1-the-consenus-problem/