

We might walk together but I run faster: Network Fairness in Blockchains



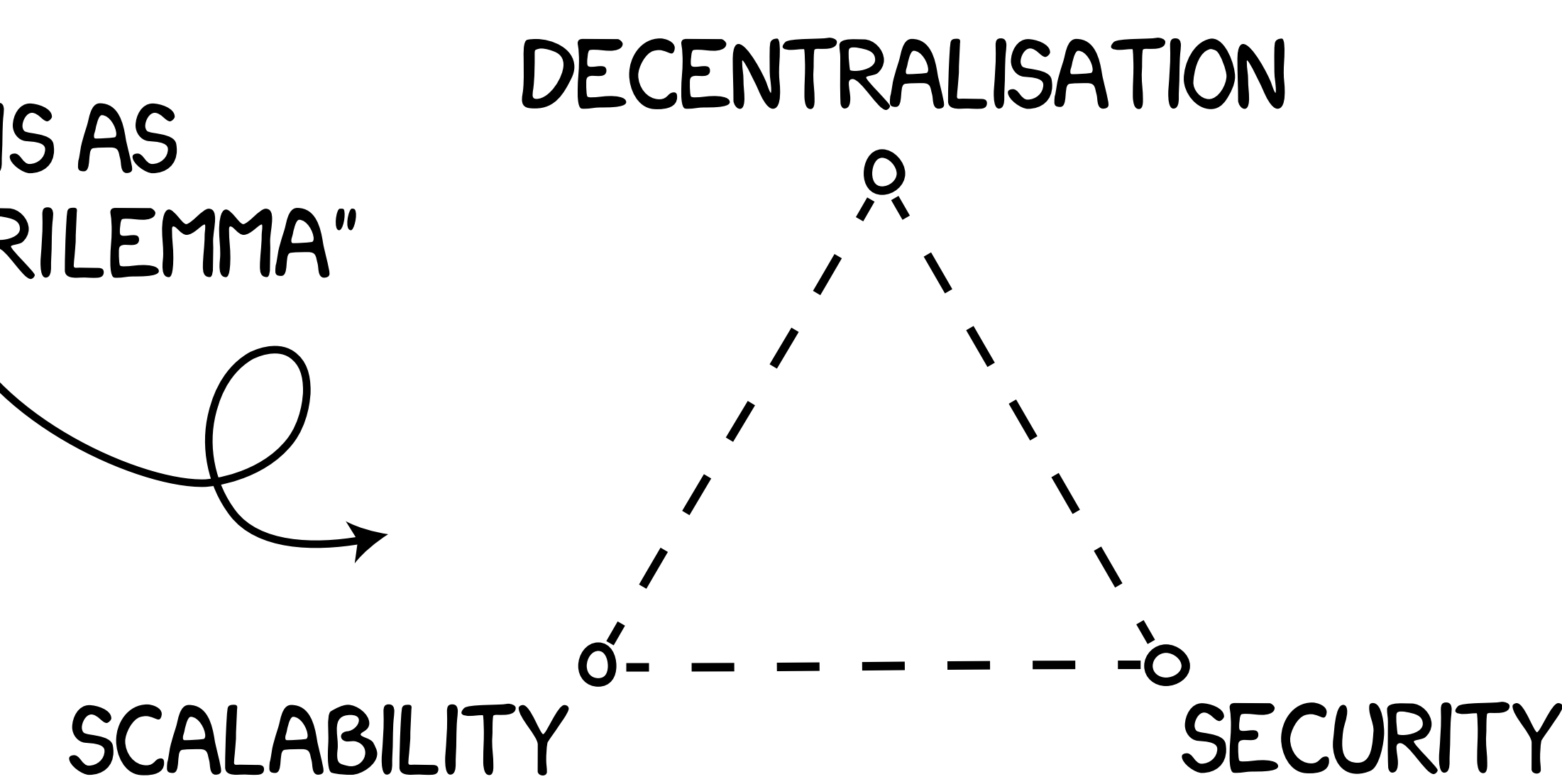
BLOCKCHAIN SCALABILITY

[2]&[3] SHOW THAT EXISTING BLOCKCHAIN PROTOCOLS SUFFER FROM A LOSS OF SECURITY PROPERTIES AS WE SCALE THEM

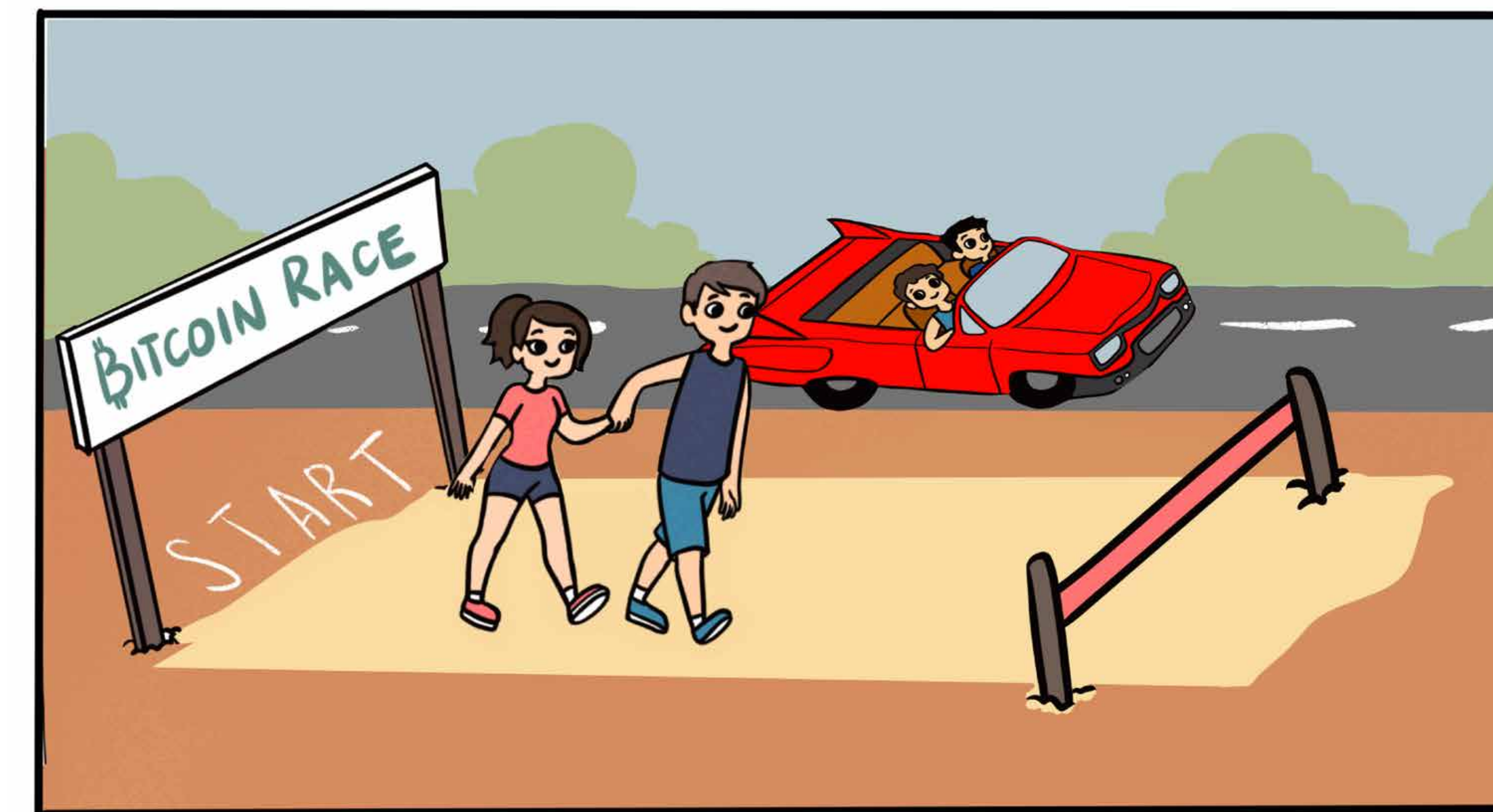
MODERN DAY CRYPTOCURRENCIES STILL LAG BEHIND CENTRALIZED PAYMENT SYSTEMS

BITCOIN	4 TX/S
ETHEREUM	10 TX/S
VISA NETWORK	1700 TX/S

VITALIK TERMED THIS AS "THE BLOCKCHAIN TRILEMMA"



IN THIS WORK, WE STUDY THE EFFECTS OF SCALING THE BLOCKCHAIN ON NETWORK FAIRNESS



NETWORK FAIRNESS

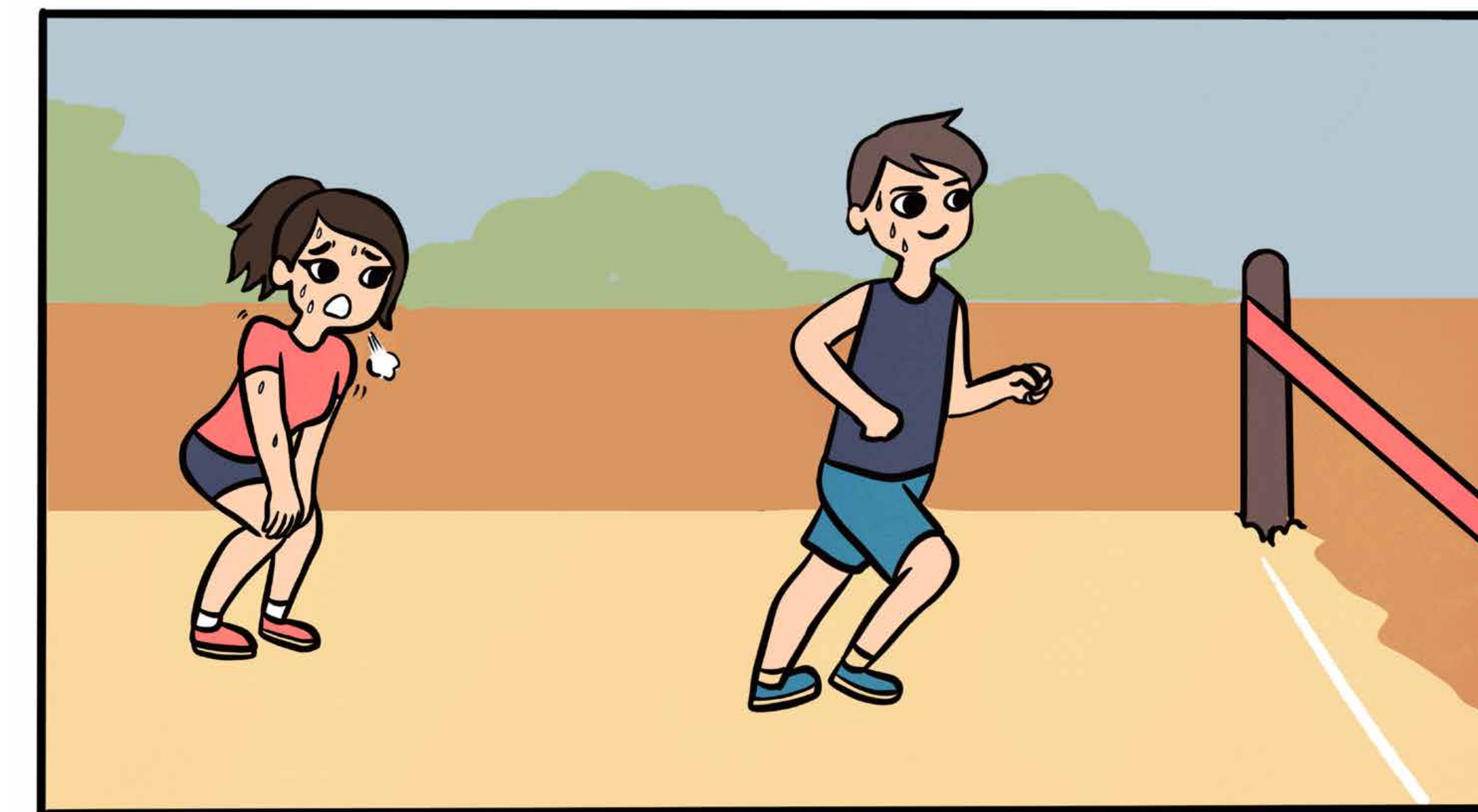
WE DEFINE TWO MEASURES OF FAIRNESS BASED ON NETWORK EVENTS

p_f - PROBABILITY OF FRONTRUNNING THAT QUANTIFIES WHETHER SLOW NODES ARE ABLE TO INCLUDE NEW TRANSACTIONS IN A BLOCK. THE HIGHER THE p_f THE LOWER THE THE PROBABILITY OF INCLUDING NEW TRANSACTIONS.

α_f - PUBLISHING FAIRNESS THAT QUANTIFIES WHETHER SLOW NODES ARE ABLE TO INCLUDE THEIR BLOCKS IN THE MAIN CHAIN

OUR KEY RESULT IS THAT BOTH THE MEASURES OF FAIRNESS DETERIORATE AS WE SCALE THE BLOCKCHAIN. THIS MAKES THE MINING OPERATION UNPROFITABLE FOR MINERS WITH SLOWER NETWORK ACCESS.

IN THE LITERATURE, IT IS TYPICALLY ASSUMED THAT ALL AGENTS HAVE EQUAL ACCESS TO THE NETWORK. FOR THE FIRST TIME, WE DROP THIS ASSUMPTION



STRATEGIC DEVIATIONS

AS THESE FAIRNESS MEASURES DETERIORATE, THE PROFITABILITY OF THE MINING OPERATION IS IMPACTED. [3] SHOW THAT A LACK OF PROFIT CAN LEAVE THE MINERS WITH TWO CHOICES :

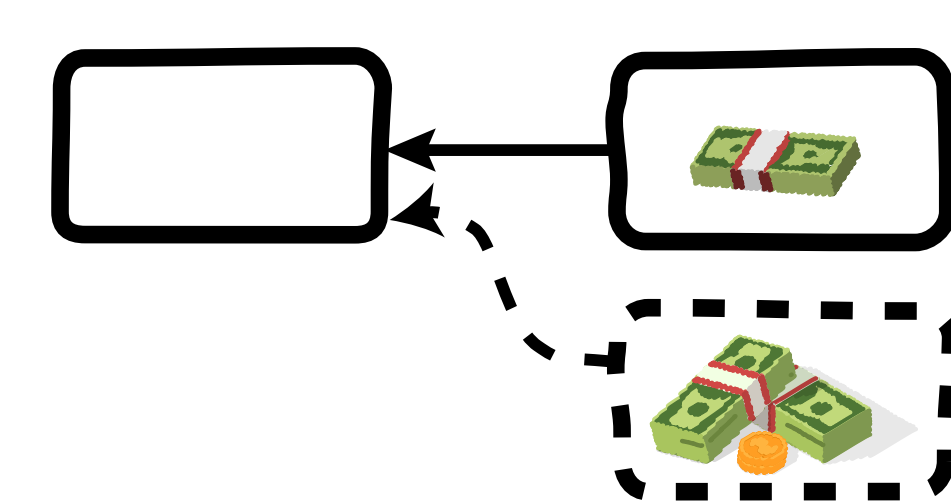
1. SHUTDOWN THE MINING OPERATION

DIRECTLY REDUCE THE HONEST COMPUTING POWER LEADING TO LOSS OF SECURITY

2. ADOPT STRATEGIC BEHAVIOR TO GAIN MORE PROFIT

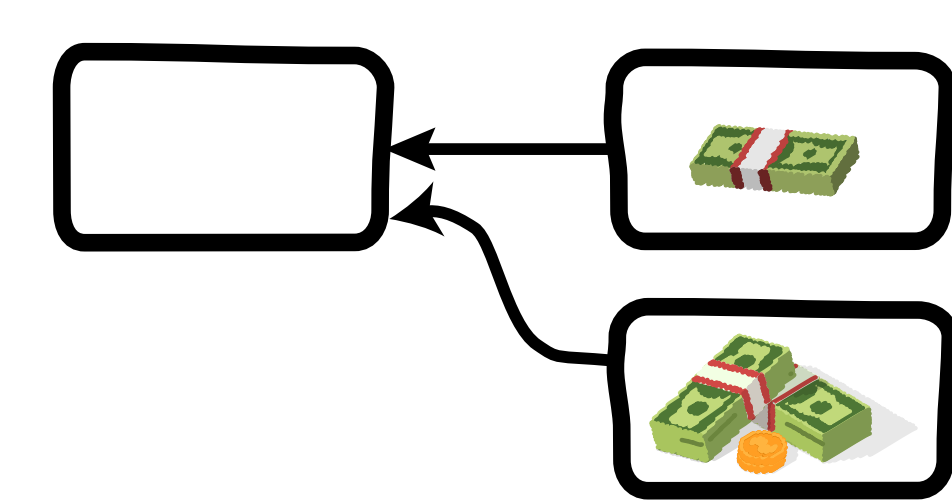
[5] PRESENT TWO SUCH STRATEGIES :

UNDERCUTTING

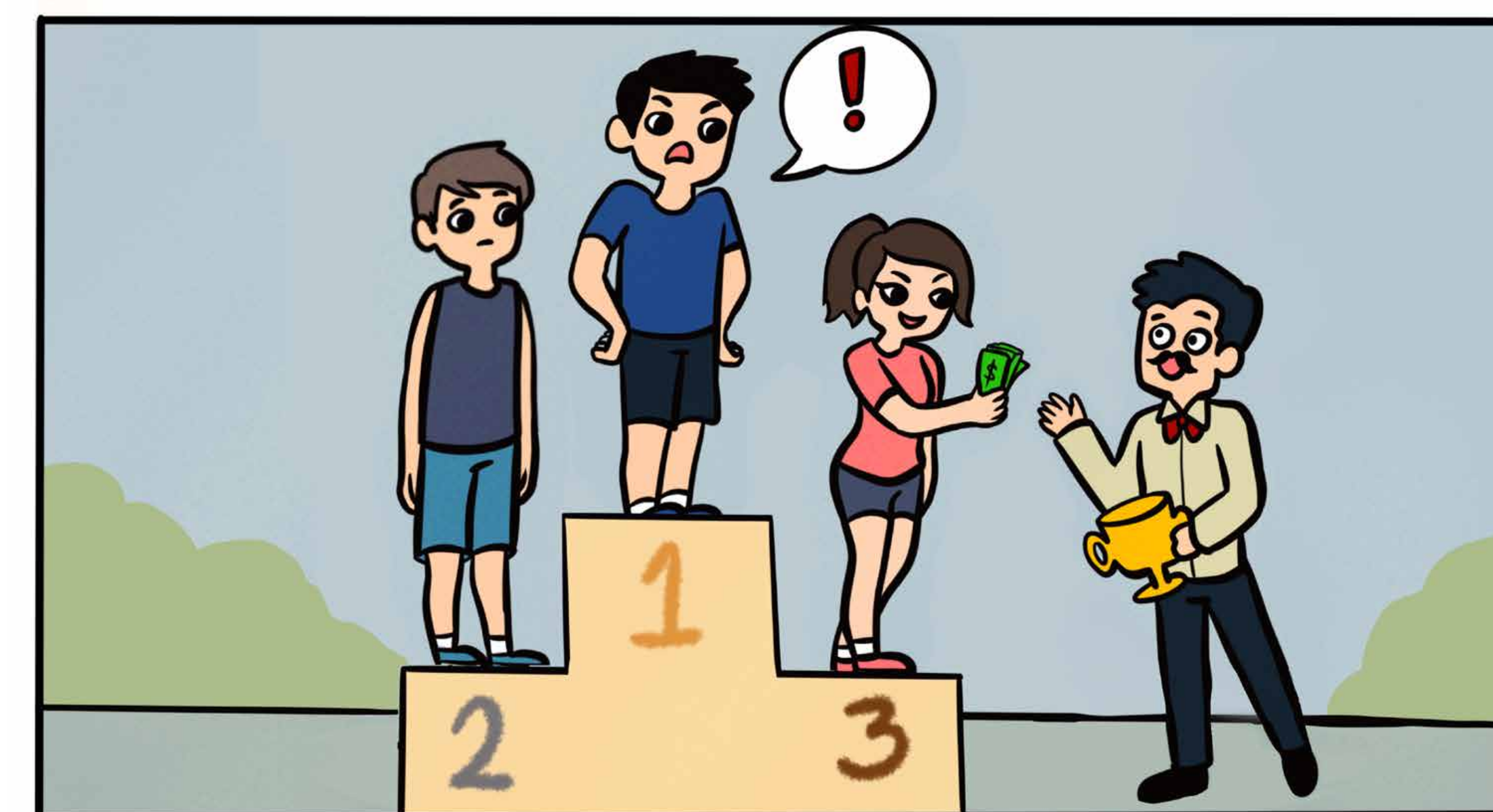


THE MINER WILL INTENTIONALLY MINE A BLOCK LEAVING OUT SOME REWARD FOR THE NEXT MINER, EFFECTIVELY OFFERING A BRIBE

PETTY MINING



IF PRESENTED A NEW BLOCK WITH HIGHER REWARD, THE MINER SWITCHES TO THE NEW BLOCK, EFFECTIVELY ACCEPTING A BRIBE



EQUILIBRIUM ANALYSIS

WE BUILT A BITCOIN MINING GAME SIMULATOR AND TESTED OUT THESE STRATEGIES AND GOT SOME PRETTY INTUITIVE BUT CONCERNING RESULTS WHEN WE INCREASE THE BLOCK CREATION RATE :

1. PETTY MINING DOMINATES OVER THE HONEST STRATEGY AN INTUITIVE RESULT, ALSO INDEPENDENTLY SHOWN BY [5]
2. IF THE FAST NODES START PETTY MINING THEN UNDERCUTTING IS THE BEST RESPONSE FOR THE SLOW NODES
3. AT THE EQUILIBRIUM, EVERY MINER TRIES TO UNDERCUT

THUS, NOT ONLY WOULD THE SECURITY BE REDUCED BUT EFFECTIVE PERFORMANCE WOULD ALSO DEGRADE

EFFECT OF STRATEGIC DEVIATIONS ON FAIRNESS: WE FOUND THAT AT THE EQUILIBRIUM, THE SLOW NODES RECEIVED AN EVEN SMALLER SHARE OF THE REVENUE. HENCE, LACK OF FAIRNESS

STRATEGIC DEVIATIONS
EVEN WORSE FAIRNESS



References:

1. Anurag Jain, Shoeb Siddiqui, and Sujit Gujar. We might walk together but I run faster: Network Fairness in Blockchains. AAMAS 2021
2. Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. EUROCRYPT 2015
3. Aggelos Kiayias and Giorgos Panagiotakos. Speed-Security Tradeoffs in Blockchain Protocols. 2015
4. Anurag Jain and Sujit Gujar. Block Rewards, Not Transaction Fees Keep Miners Faithful In Blockchain Protocols. GTIB@WINE2020
5. Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. On the instability of bitcoin without the block reward. CCS 2016



Download

Work done at:



Machine Learning Lab

Authors: Anurag Jain, Shoeb Siddiqui, Prof. Sujit Gujar
Research Center: Machine Learning Lab (MLL)
Email ID: anurag.jain@research.iiit.ac.in



Poster presented at:

