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

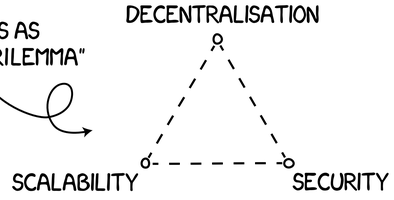
Anurag Jain, Shoeb Siddiqui and Sujit Gujar

International Institute of Information Technology, Hyderabad, India (IIIT-H)

BLOCKCHAIN SCALABILITY

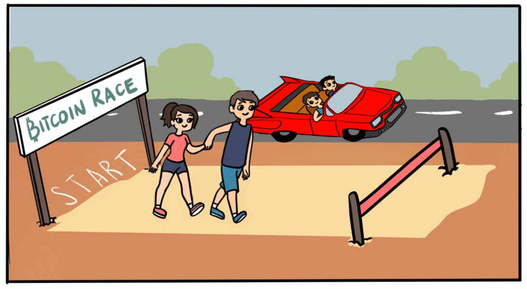
[1]&[2] SHOW THAT EXISTING BLOCKCHAIN PROTOCOLS SUFFER FROM A LOSS OF SECURITY PROPERTIES AS WE SCALE THEM

VITALIK TERMED THIS AS "THE BLOCKCHAIN TRILEMMA"



MODERN DAY CRYPTOCURRENCIES STILL LAG BEHIND CENTRALIZED PAYMENT SYSTEMS

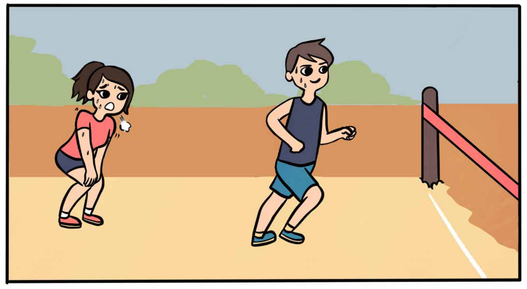
BITCOIN	4 TX/S
ETHEREUM	10 TX/S
VISA NETWORK	1700 TX/S



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

NETWORK FAIRNESS

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



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

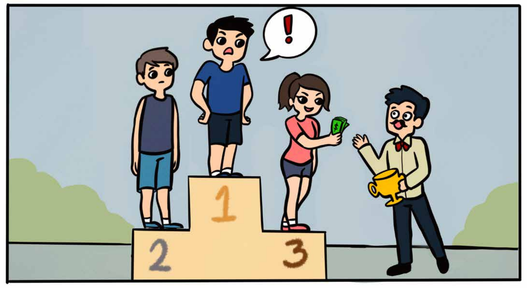
OUR KEY RESULT IS THAT BOTH THE MEASURES OF FAIRNESS DETERIORATE AS WE SCALE THE BLOCKCHAIN. THIS MAKES THE MINING OPERATION UNPROFITABLE FOR MINERS WITH SLOWER NETWORK ACCESS.

STRATEGIC DEVIATIONS

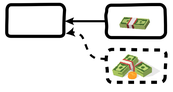
AS THESE FAIRNESS MEASURES DETERIORATE, THE PROFITABILITY OF THE MINING OPERATION IS IMPACTED. [3] SHOW THAT A LACK OF PROFIT CAN LEAVE THE MINERS WITH TWO CHOICES :

1. SHUTDOWN THE MINING OPERATION
   - DIRECTLY REDUCE THE HONEST COMPUTING POWER LEADING TO LOSS OF SECURITY
2. ADOPT STRATEGIC BEHAVIOR TO GAIN MORE PROFIT

[4] PRESENT TWO SUCH STRATEGIES :



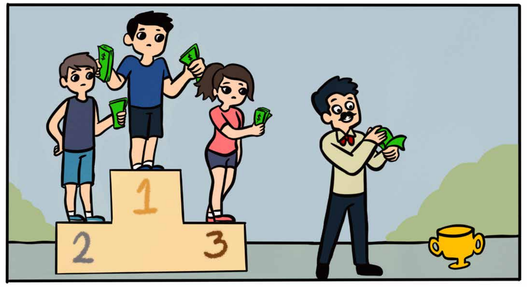
UNDERCUTTING



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



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

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

References:

1. Juan Garay, Aggelos Kiayias, and Nikos Leonardos. 2014. The Bitcoin Backbone Protocol: Analysis and Applications.
2. Aggelos Kiayias and Giorgos Panagiotakos. 2015. Speed-Security Tradeoffs in Blockchain Protocols.
3. Anurag Jain and Sujit Gujar. 2020. Block Rewards, Not Transaction Fees Keep Miners Faithful In Blockchain Protocols
4. Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. 2016. On the instability of bitcoin without the block reward.

Work done at:

Machine Learning Lab

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Poster presented at:

AAMAS2021 ONLINE, MAY 3–7