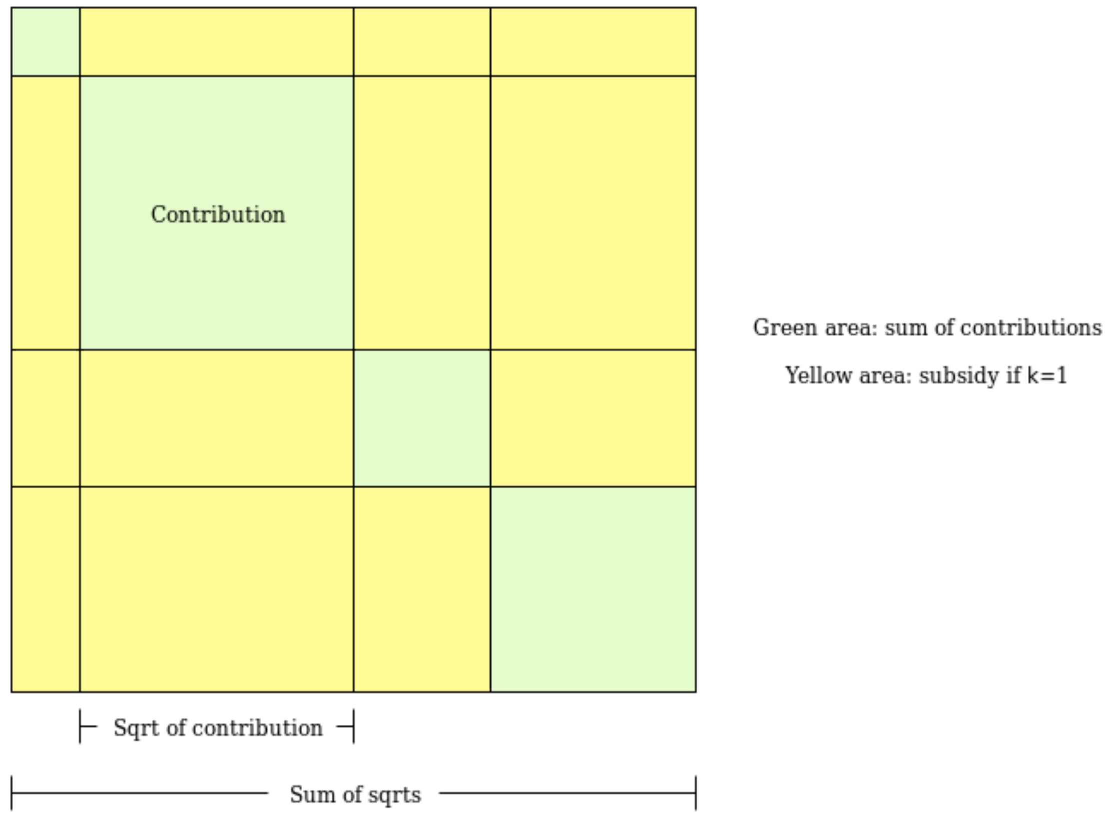
MACI @ ETHDenver

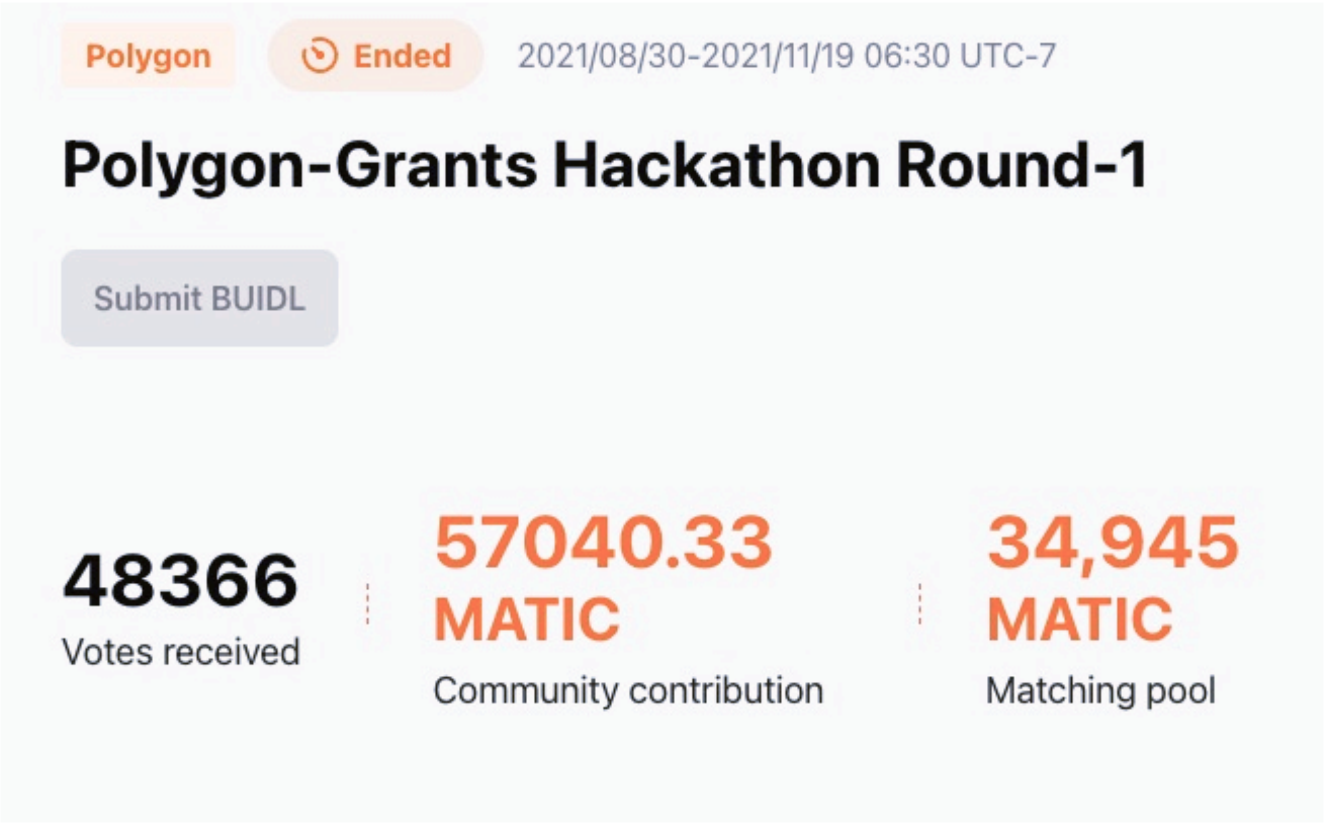
Eric @DoraHacks
Schelling Point Event

2022.2.17

QV / QF: Solving Tragedy of the Commons

Heavy mix of theory and empirical practices




Polygon Ended 2021/08/30-2021/11/19 06:30 UTC-7

Polygon-Grants Hackathon Round-1

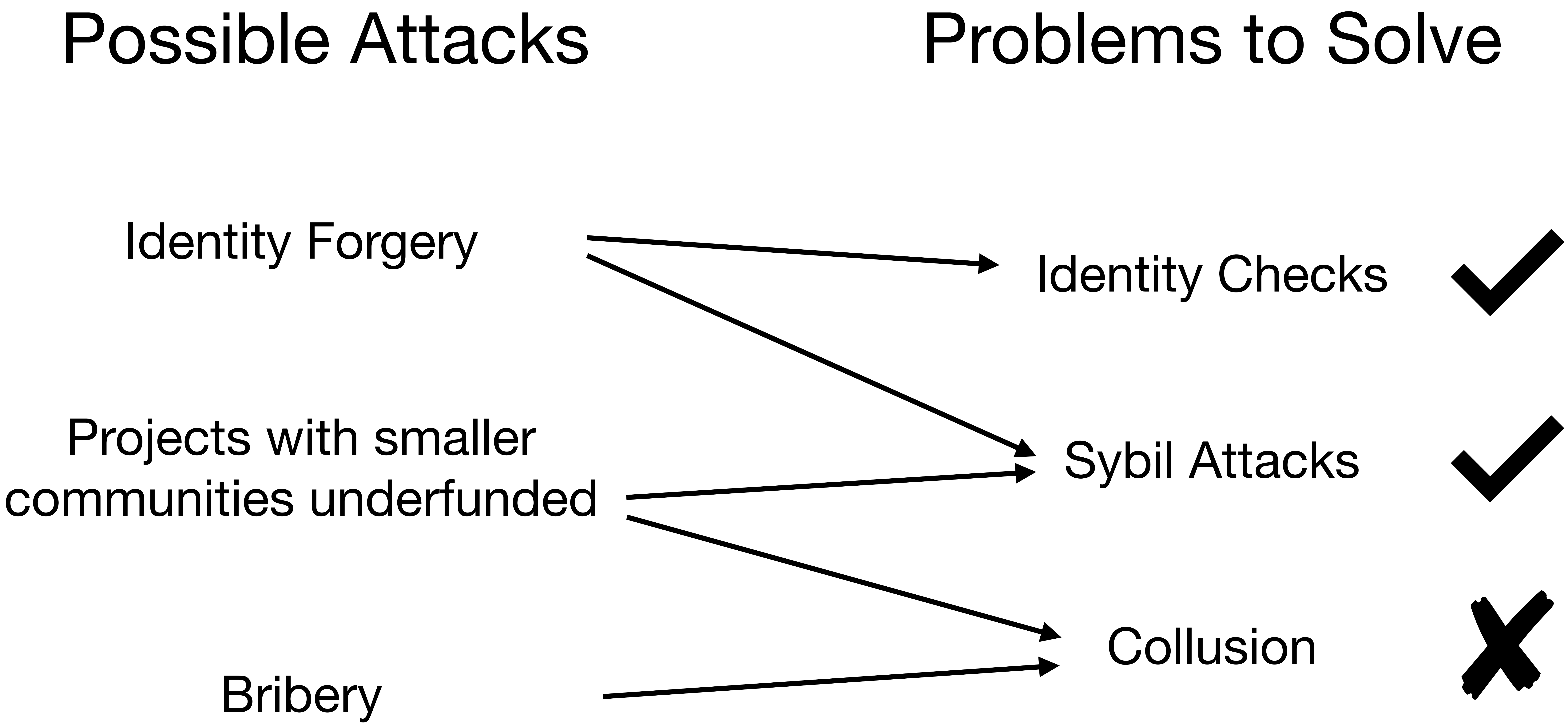
Submit BUIDL

48366	57040.33 MATIC	34,945 MATIC
Votes received	Community contribution	Matching pool

Fairness <-> System Security <-> Scaling

https://vitalik.ca/general/2019/12/07/quadratic.html

https://hackerlink.io/grant/polygon/top



Possible Attacks

Identity Forgery

Projects with smaller communities underfunded

Bribery

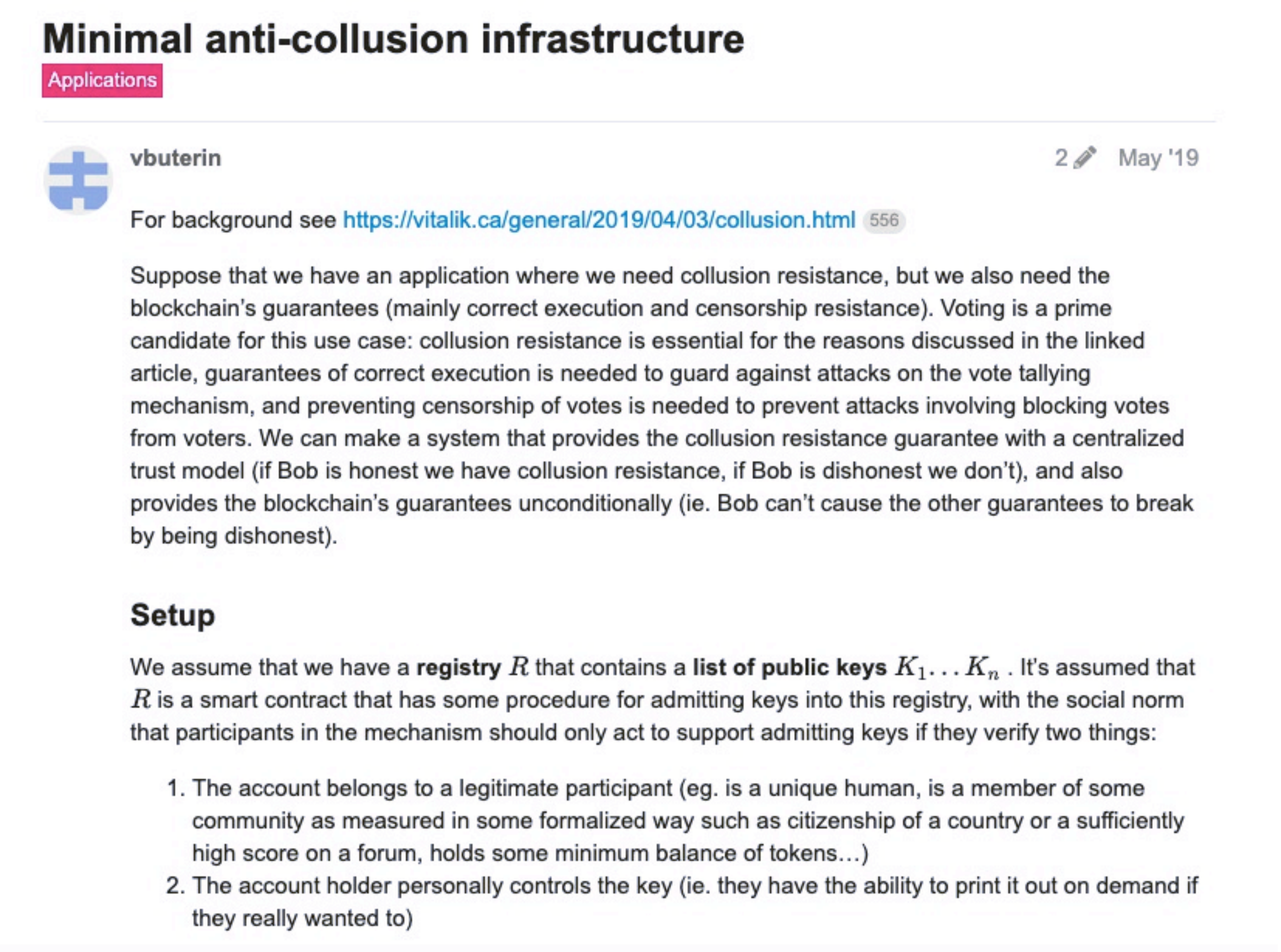
Problems to Solve

Identity Checks ✓

Sybil Attacks ✓

Collusion ✗

Vitalik: MACI!



Minimal anti-collusion infrastructure

Applications

vbuterin 2 May '19

For background see https://vitalik.ca/general/2019/04/03/collusion.html 556

Suppose that we have an application where we need collusion resistance, but we also need the blockchain's guarantees (mainly correct execution and censorship resistance). Voting is a prime candidate for this use case: collusion resistance is essential for the reasons discussed in the linked article, guarantees of correct execution is needed to guard against attacks on the vote tallying mechanism, and preventing censorship of votes is needed to prevent attacks involving blocking votes from voters. We can make a system that provides the collusion resistance guarantee with a centralized trust model (if Bob is honest we have collusion resistance, if Bob is dishonest we don't), and also provides the blockchain's guarantees unconditionally (ie. Bob can't cause the other guarantees to break by being dishonest).

Setup

We assume that we have a **registry** R that contains a **list of public keys** $K_1 ... K_n$. It's assumed that R is a smart contract that has some procedure for admitting keys into this registry, with the social norm that participants in the mechanism should only act to support admitting keys if they verify two things:

1. The account belongs to a legitimate participant (eg. is a unique human, is a member of some community as measured in some formalized way such as citizenship of a country or a sufficiently high score on a forum, holds some minimum balance of tokens…)
2. The account holder personally controls the key (ie. they have the ability to print it out on demand if they really wanted to)

https://ethresear.ch/t/minimal-anti-collusion-infrastructure/5413

MACI @ ETHDenver

Feb 20 SUN

8:00am Submission ddl @ hackerlink.io
3:00pm 30 finalists announced
MACI community voting start
6:00pm MACI round ends
7:45pm Community voting result announced
Proofs uploaded

hackerlink.io/grant/ethdenver22

Related Efforts to Check Out

MACI Anonymization

https://ethresear.ch/t/adding-anonymization-to-maci/6329

https://ethresear.ch/t/maci-anonymization-using-rerandomizable-encryption/7054

MACI 1.0 @PrivacyScaling

clr.fund (from ETHDenver 21)