

# Enhancing Cryptocurrency Blocklisting: A Secure, Trustless, and Effective Realization

*Yuefeng Du, Anxin Zhou, Cong Wang*

City University of Hong Kong

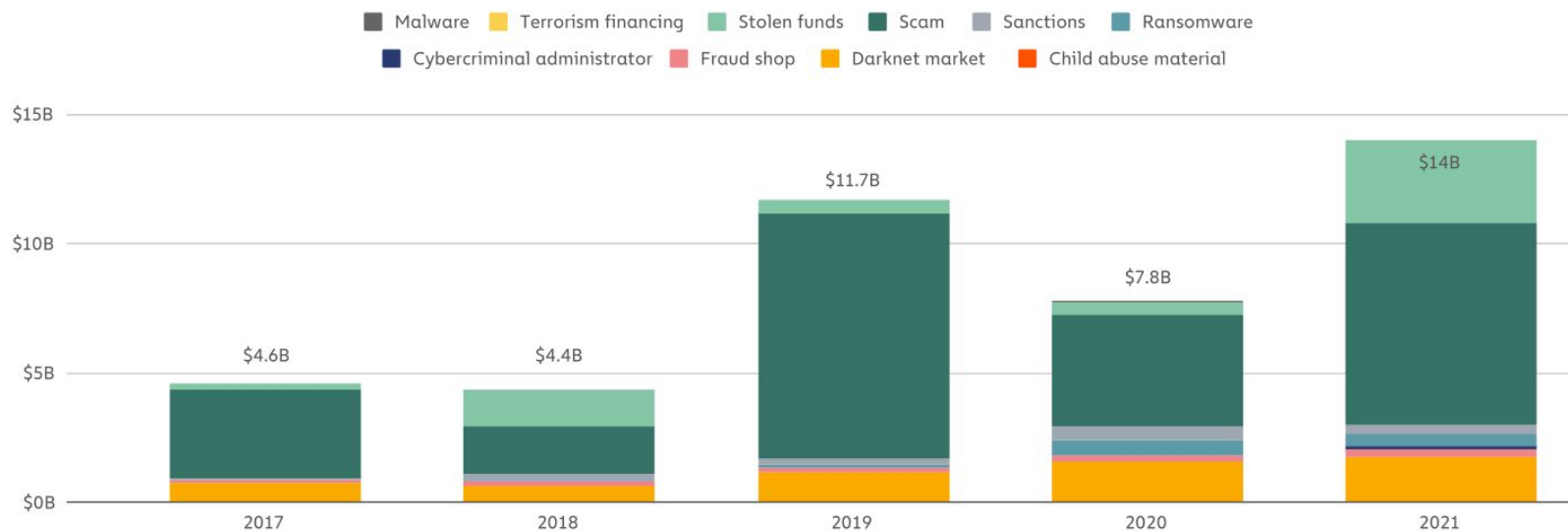


香港城市大學  
City University of Hong Kong

專業 創新 胸懷全球  
Professional · Creative  
For The World

# Prevalent Cryptocurrency Crimes

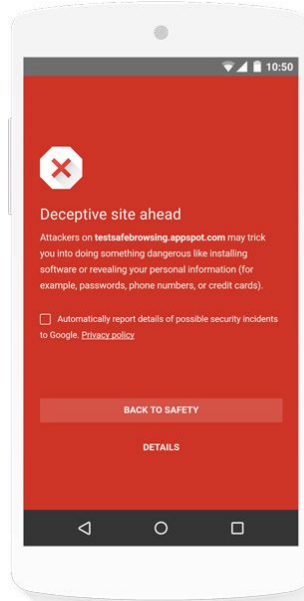
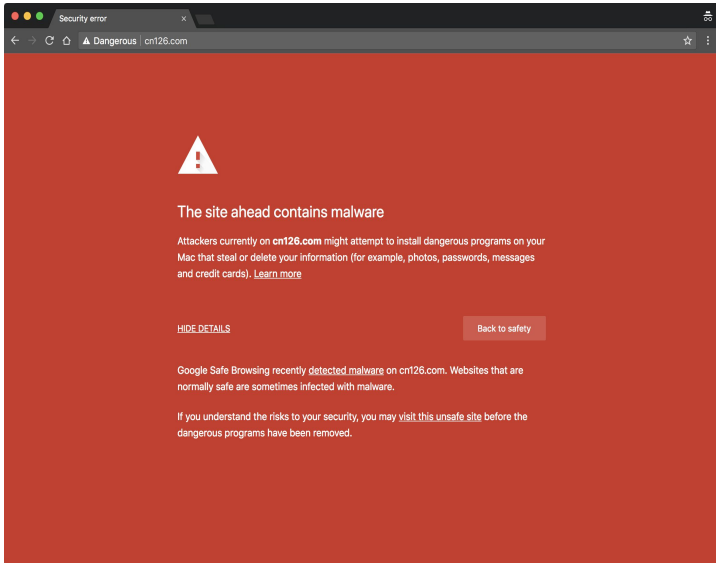
## Total cryptocurrency value received by illicit addresses | 2017–2021



*Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.*

**Figure taken from The 2022 Crypto Crime Report, Chainalysis**

# Safe Browsing: URL Blocklisting



Block **malware** or **phishing**

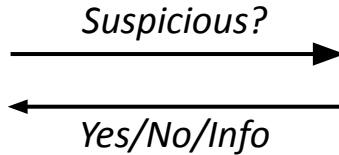
- **Chrome, Firefox, Safari ...**
- **4 billions** devices

# Safe Transaction: Cryptocurrency Blocklisting

Client



Blockchain  
account/address

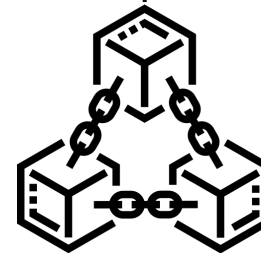


List of  
unsafe addresses

Blocklist Service



*Data mining*



Blockchain Records

Address 0xf52baeb41abf6a9001f42246d5a3a9e2677bc8f5

Upbit Hack

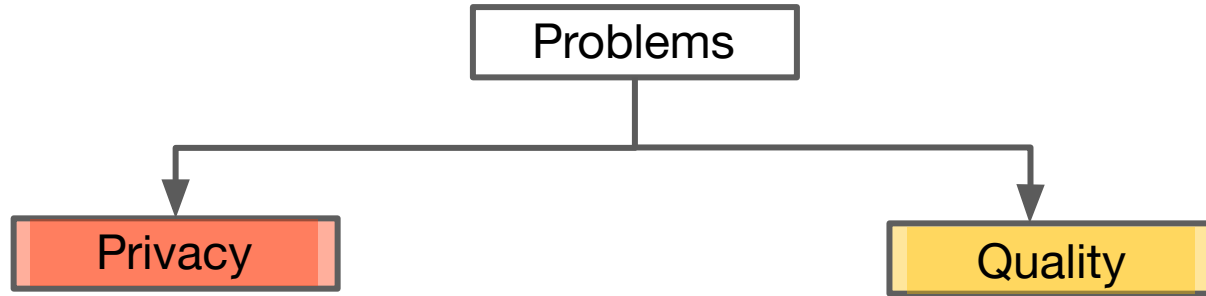
Feature Tip: DEFI - Track your Compound & Maker loans on Etherscan!

Warning! This address received funds from an address that is associated to Upbit's Exchange Hack. Please exercise caution when interacting with this address.

Overview	Upbit Hacker 3.3	More Info
Balance:	7,986.902942108 Ether	My Name Tag: Not Available, login to update
Ether Value:	\$1,266,163.72 (@ \$158.53/ETH)	
Token:	\$4.55	

**ETHProtect** warns **Etherscan** users of phishing, scams, and hacks.

# Problems with Cryptocurrency Blocklisting



## Problem #1: Privacy

- Blocklist service providers see sensitive user queries in the clear
  - Facilitate data collection & user profiling
  - Leak user intention (e.g., frontrunning attacks, forcing up tx fee, DoS)

## Problem #1: Privacy

- Blocklist service providers see sensitive user queries in the clear
  - Facilitate data collection & user profiling
  - Leak user intention (e.g., frontrunning attacks, forcing up tx fee, DoS)
- Blocklists are proprietary assets by the service providers
  - Should avoid disclosure to unauthorized parties

# Problem #1: Privacy

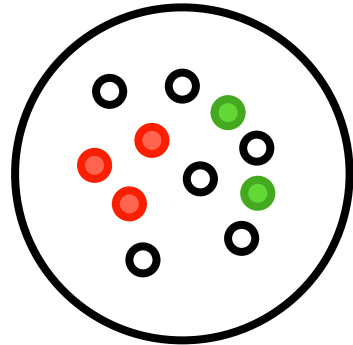
- ▶ Blocklist servers see sensitive user queries in the clear
- ▶ Facilitate data collection user profiling
- ▶ Leak

**Goal:** Enable privacy-preserving blocklist queries for cryptocurrency addresses

Transaction Action:	Remove 2,193,612,748.362 96682864463661133 SHIB And 13,291,13354374433308011 Ether Liquidity From Uniswap V2																				
From:	0xab5801a7d398351b8be11c439e05c5b3259aec9b (Vb)																				
Interacted With (To):	Contract 0x7a250d5630b4cf539739df2c5dadb4c6692488d (Uniswap V2/ Router 2) TRANSFER 13,291,13354374433308011 Ether From Wrapped Ether To Uniswap V2: Rou... TRANSFER 13,291,13354374433308011 Ether From Uniswap V2: Rou... To Vb																				
Tokens Transferred:	<table><tr><td>From Vb</td><td>To Uniswap V2: SHIB</td><td>For 70,356,236,397351443318463451 (\$187,491,752.73)</td><td>Uniswap V2 (UNI-V2)</td></tr><tr><td>From Uniswap V2: SHIB</td><td>To Null Address: 0x00...</td><td>For 70,356,236,397351443318463451 (\$187,491,752.73)</td><td>Uniswap V2 (UNI-V2)</td></tr><tr><td>From Uniswap V2: SHIB</td><td>To Uniswap V2: Rout...</td><td>For 2,193,612,748,362,96682864463661133 (\$24,063,931.85)</td><td>SHIBA INU (SHIB)</td></tr><tr><td>From Uniswap V2: SHIB</td><td>To Uniswap V2: Rout...</td><td>For 13,291,13354374433308011 (\$24,243,957.86)</td><td>Wrapped Ethe... (WETH)</td></tr><tr><td>From Uniswap V2: Rout...</td><td>To Vb</td><td>For 2,193,612,748,362,96682864463661133 (\$24,063,931.85)</td><td>SHIBA INU (SHIB)</td></tr></table>	From Vb	To Uniswap V2: SHIB	For 70,356,236,397351443318463451 (\$187,491,752.73)	Uniswap V2 (UNI-V2)	From Uniswap V2: SHIB	To Null Address: 0x00...	For 70,356,236,397351443318463451 (\$187,491,752.73)	Uniswap V2 (UNI-V2)	From Uniswap V2: SHIB	To Uniswap V2: Rout...	For 2,193,612,748,362,96682864463661133 (\$24,063,931.85)	SHIBA INU (SHIB)	From Uniswap V2: SHIB	To Uniswap V2: Rout...	For 13,291,13354374433308011 (\$24,243,957.86)	Wrapped Ethe... (WETH)	From Uniswap V2: Rout...	To Vb	For 2,193,612,748,362,96682864463661133 (\$24,063,931.85)	SHIBA INU (SHIB)
From Vb	To Uniswap V2: SHIB	For 70,356,236,397351443318463451 (\$187,491,752.73)	Uniswap V2 (UNI-V2)																		
From Uniswap V2: SHIB	To Null Address: 0x00...	For 70,356,236,397351443318463451 (\$187,491,752.73)	Uniswap V2 (UNI-V2)																		
From Uniswap V2: SHIB	To Uniswap V2: Rout...	For 2,193,612,748,362,96682864463661133 (\$24,063,931.85)	SHIBA INU (SHIB)																		
From Uniswap V2: SHIB	To Uniswap V2: Rout...	For 13,291,13354374433308011 (\$24,243,957.86)	Wrapped Ethe... (WETH)																		
From Uniswap V2: Rout...	To Vb	For 2,193,612,748,362,96682864463661133 (\$24,063,931.85)	SHIBA INU (SHIB)																		

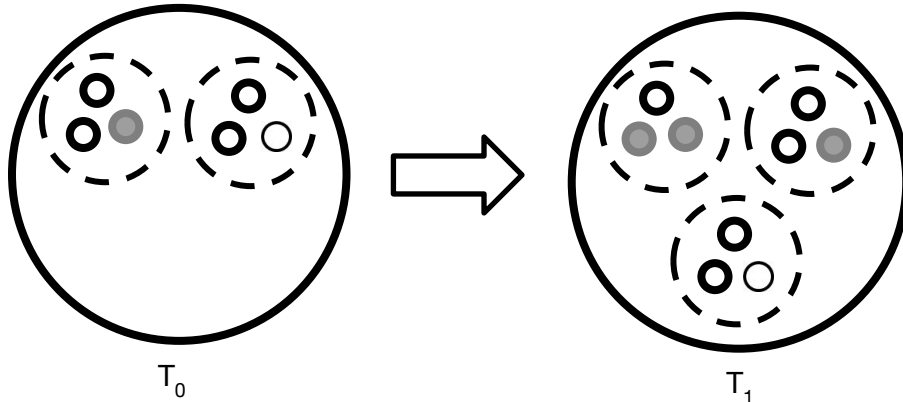


## Problem #2: Quality



- Real threats unrecognized  
unintendedly /deliberately
- Safe addresses  
mis-identified as dangerous  
ones.

- Blocklists can be
  - Diverse
  - Inaccurate [1]
  - Evolving [2]



- [1] BLAG: Improving the Accuracy of Blacklists, Ramanathan et al., In Proc. of NDSS, 2020.  
[2] Blocklist babel: On the transparency and dynamics of open source blocklisting, Feal et al., IEEE Trans. Netw. Serv. Manag. 18(2), 2021

## Problem #2: Quality

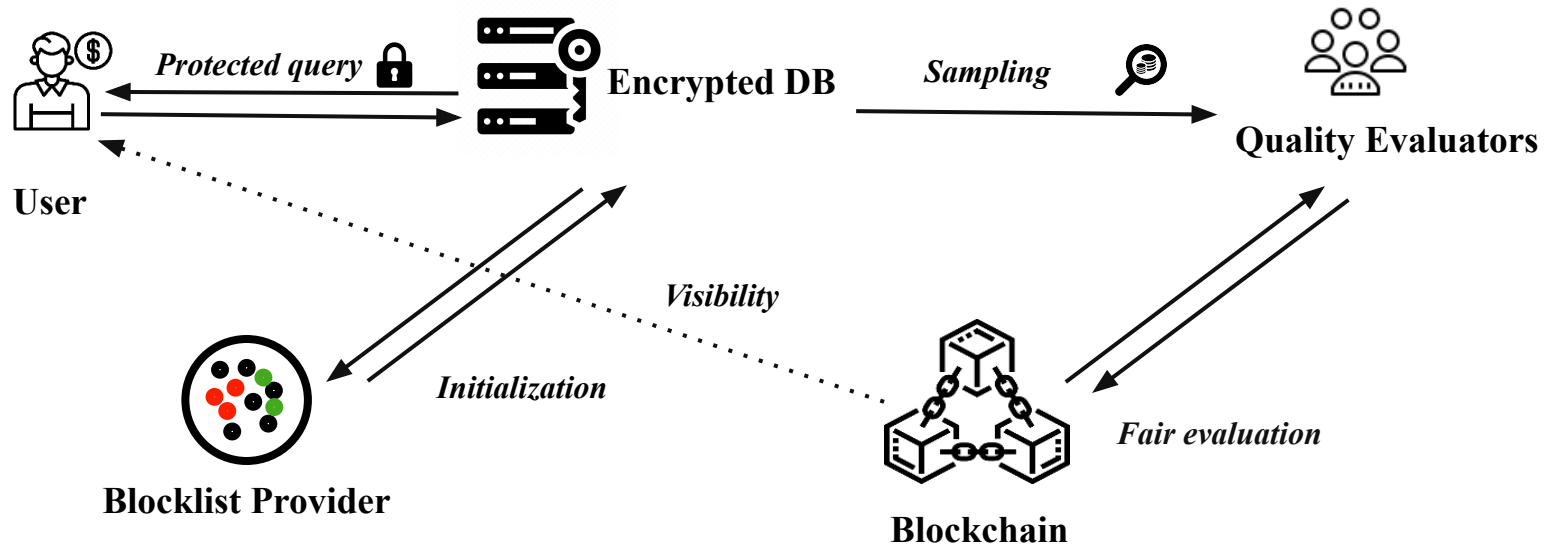
● Real threats unrecognized  
unintended / deliberately

● Blocklists can be  
○ Inconsistent

**Goal:** Ensure high-quality blacklist services with a proper quality evaluation mechanism

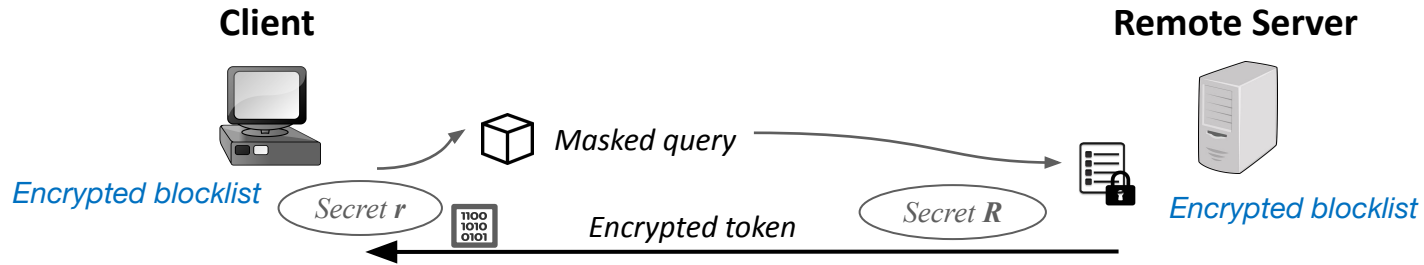
1. BLAG: Improving the Accuracy of Blacklists, Ramanathan et al., In Proc. of NDSS, 2020.
2. Blocklist babel: On the transparency and dynamics of open source blocklisting, Feal et al., IEEE Trans. Netw. Serv. Manag. 18(2), 2021

# Our architecture



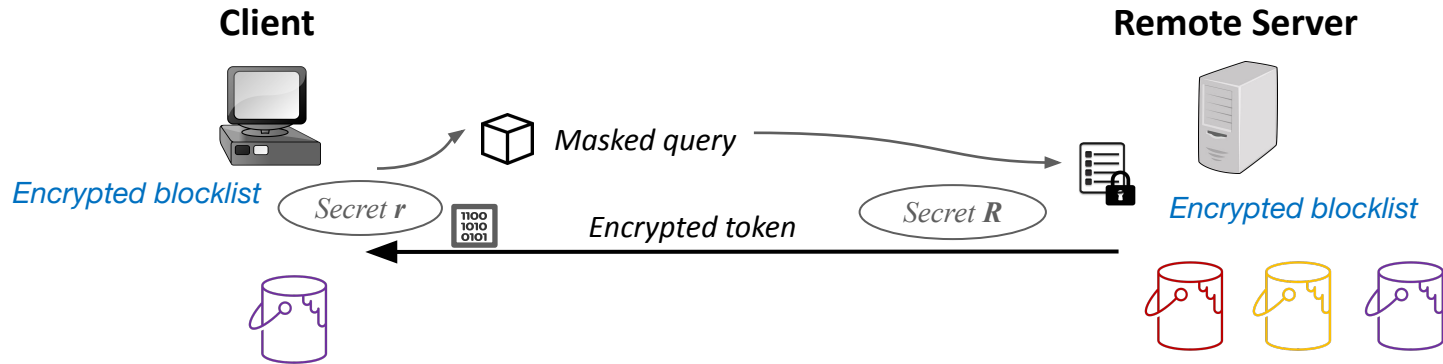
- Decoupling the curation and serving of blocklists
- Decentralized evaluation of blocklist quality

# Addressing Problem #1: Private Query



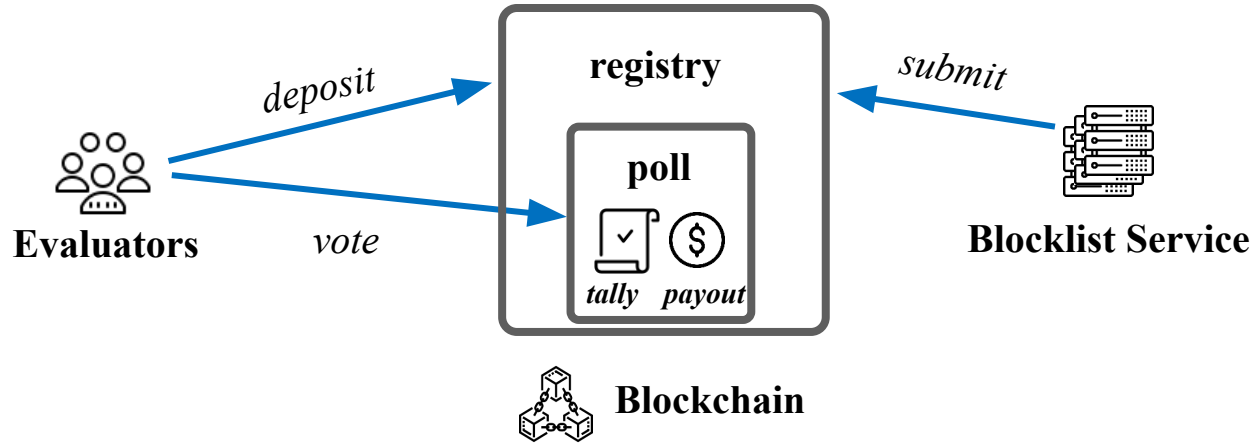
- Goal: same query complexity as the existing blocklist services
  - One round-trip per query, precluding the hefty crypto primitives like PIR
- We propose to store an encrypted (and searchable) blocklist at the client side
  - Client asks server for authorised search tokens

# Addressing Problem #1: Private Query



- Goal: same query complexity as the existing blocklist services
  - One round-trip per query, precluding the hefty crypto primitives like PIR
- We propose to store an encrypted (and searchable) blocklist at the client side
  - Client asks server for authorised search tokens
- Further enhancement:
  - Use bucketization for large list; more friendly for fresh update

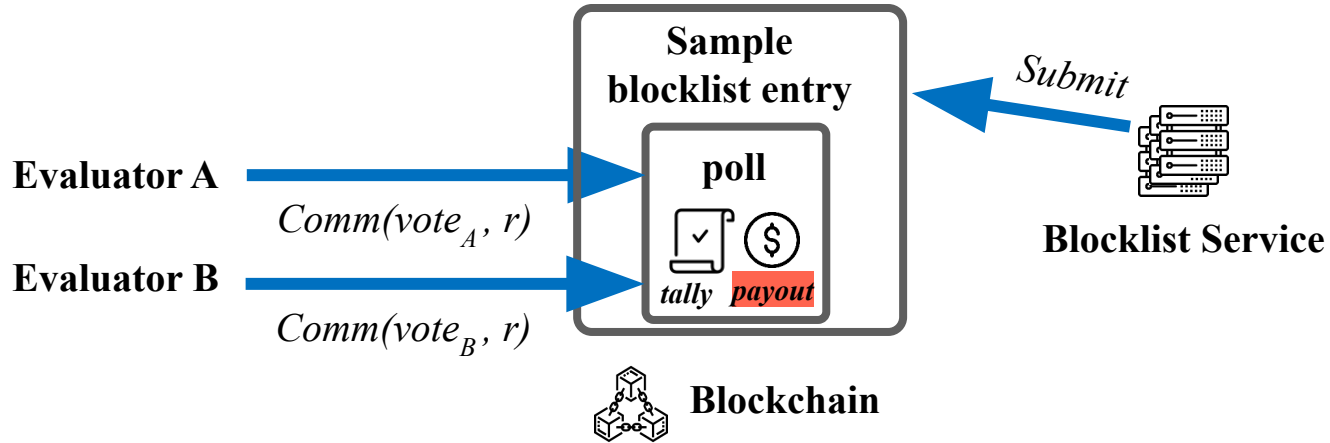
## Addressing Problem #2: Decentralized Fair Blocklist Evaluation



- Inspired by Token Curated Registry (TCR) [1]
  - “Stake, and then vote for what you will use”
    - Vote weight proportional to stake
  - Assumption: economically rational participants

[1] Token curated registries - a game theoretic approach, Asgaonkar et. al., arXiv, 2018.

# Challenge: Fair Evaluation

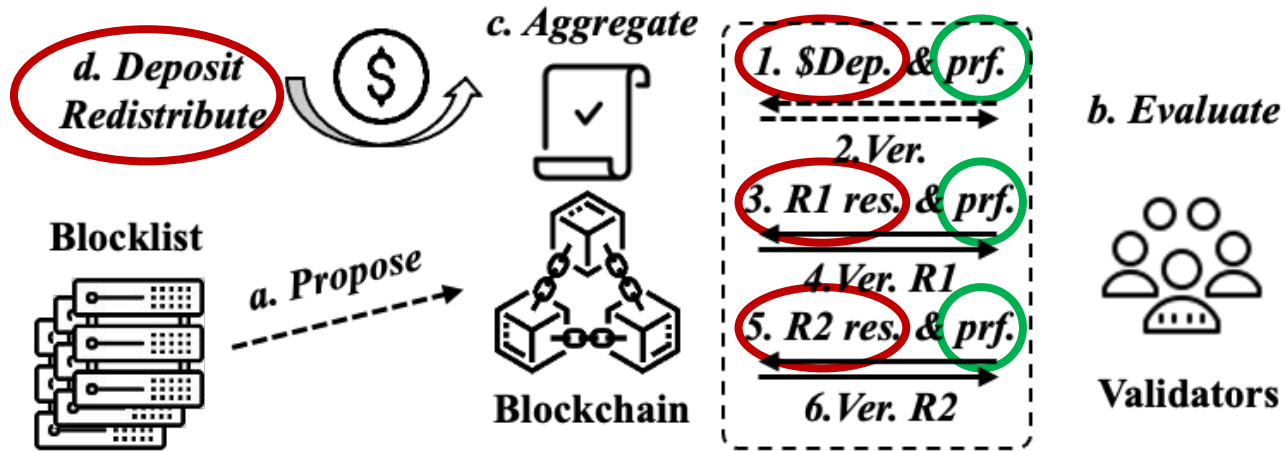


- The existing TCR practice is known to produce unfair results:
  - **Biased outcome** due to revealing order [1]
  - **Coercion** out of economic incentives [2]

[1] SHARVOT: secret SHARe-based Voting on the blockchain, Bartolucci et. al., Proc. of ICSE, 2018.

[2] Quadratic Voting in Blockchain Governance., Nicola Dimitri, *Information* 2022.

# Resistance to Bias: Zero-Knowledge Evaluation



- ▶ **Vote & stake confidentiality is a must**

- ▶ No disclosure of (intermediate) outcome, e.g., \$deposit, Round 1 & Round 2 results

- ▶ **Low-cost public verification**

- ▶ Detect any behavior deviation with minimized on-chain costs



# Resistance to Coercion



## Coercion-resistant voting:

- ▶ Well studied in cooperative game theory, e.g., Stackelberg competition
- ▶ Goal: maximize the costs of coercion to disincentivize attacks

- ▶ Real-world incidents:
  - ▶ e.g., Dark DAO, Curve War

# Resistance to Coercion: Cryptographic Sortition



- Real-world incidents:
  - e.g., Dark DAO, Curve War

## Coercion-resistant voting:

- Well studied in cooperative game theory, e.g., Stackelberg competition
- Goal: maximize the costs of coercion to disincentivize attacks
- We further extend the TCR design
  - Enlarge the candidate pool for evaluators
  - Secure random evaluator selection
    - Inspired by cryptographic sortition [1]
    - We adapt it to **encrypted values**

[1] Algorand: Scaling Byzantine Agreements for Cryptocurrencies, Gilad et.al., in Proc of SOSP, 2017

## Evaluation Setup

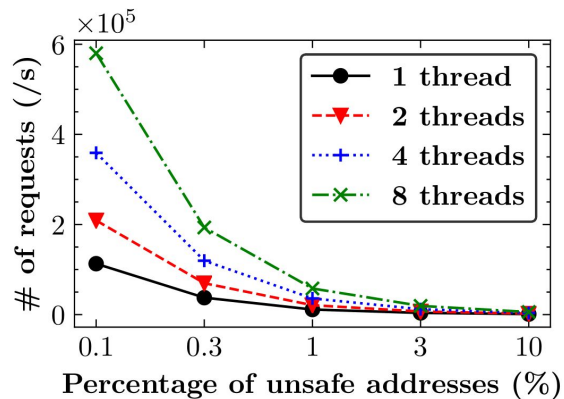
- Real-world blocklists (over 240,000 entries)
- Ethereum for decentralized blocklist evaluation
- 10-20 evaluators



# Overhead of Private Query

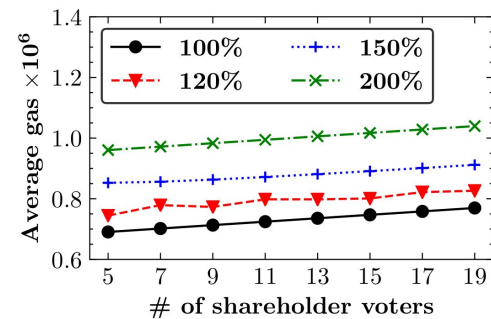
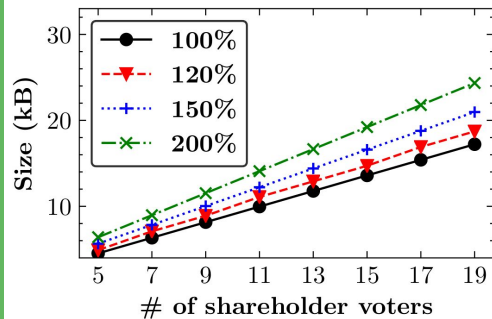
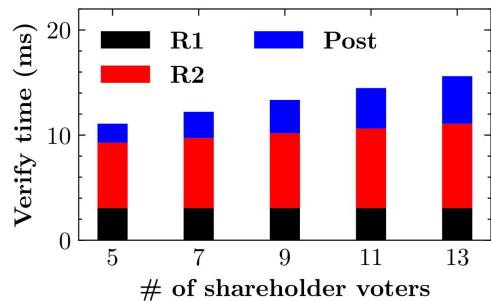
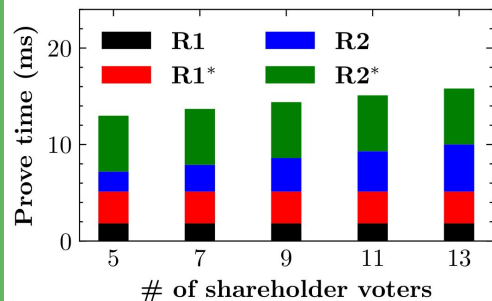
Prefix len.	Sec. wrt. $k$	Resp. size ( $kB$ )
16 bit	4	0.13
8 bit	977	30.53

Orac. $H$	Preprocess time <sup>†</sup>	Qry. time ( $ms$ )
Sha256	$1.55 \pm 0.02$ sec.	$0.38 \pm 5 \times 10^{-3}$
Argon2*	$1.27 \pm 0.03$ hour	$147.29 \pm 4.26$



- Tunable security guarantees and communication overhead
- Practical initialization and query cost
- Throughput is affected by %unsafe addresses

# Costs of Blocklist Evaluation



# of shareholder voters	5	7	9	11
Cost (USD)	16.02	16.28	16.54	16.80

Estimated on-chain cost undertaken by each evaluator

- Off-chain computation time
- On-chain costs
  - Proof storage
  - Ethereum gas for on-chain verification
- All linear to #evaluators

## Concluding Remarks

- Two major problems in cryptocurrency blocklisting
  - No protection of sensitive queries
  - No (trustless) guarantee of blocklist quality
- Our solution raises the bar on privacy and security of this booming ecosystem

## Concluding Remarks

- Two major problems in cryptocurrency blocklisting
  - No protection of sensitive queries
  - No (trustless) guarantee of blocklist quality
- Our solution raises the bar on privacy and security of this booming ecosystem



# Commit-and-Prove Zero Knowledge Proof



Bob

Prove it in Zero Knowledge then...



Alice

I know a solution, but I don't want to tell you!

Revealing nothing but the correctness of committed values

▸ *Partial vote confidentiality*

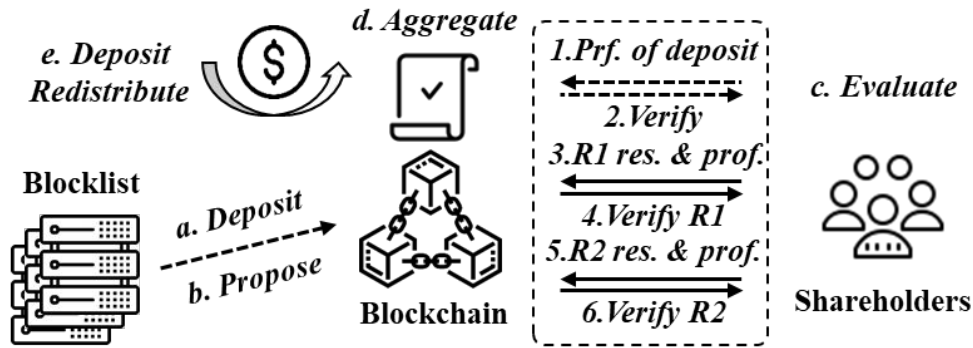


▸ *Public verifiability*





# Construction Explained at a High Level



$$Q = \begin{cases} 1, & \sum_{i=0}^{n-1} \tau_i v_i > \frac{1}{2} \sum_{i=0}^{n-1} \tau_i \\ 0, & \sum_{i=0}^{n-1} \tau_i v_i \leq \frac{1}{2} \sum_{i=0}^{n-1} \tau_i \end{cases}$$

We consider a scenario where only 1-bit outcome is revealed lastly.

$Q$  is revealed by tally and decommit  $Y$

*Deposit:*

$$\begin{aligned} r &\leftarrow \$ F \\ C &\leftarrow g^{\text{amount}} h^r \\ \mathbf{prf}_0 &\leftarrow \text{NIZK.Prove}(R_{\text{dep}}, C, r) \end{aligned}$$

*R1:*

$$\begin{aligned} \text{comm}_0, \text{comm}_1 &\leftarrow (g^r, g^{\text{vote}} h^r) \\ \mathbf{prf}_1 &\leftarrow \text{NIZK.Prove}(R_1, \text{comm}_0, r) \end{aligned}$$

*R2:*

$$\begin{aligned} Y &\leftarrow \prod_{i=0}^{p-1} \text{comm}_{i,0}^{g^{\text{vote}}} / \prod_{i=p+1}^{N-1} \text{comm}_{i,0} \\ \mathbf{prf}_2 &\leftarrow \text{NIZK.Prove}(R_2, \text{comm}_1, (\text{vote}, r)) \end{aligned}$$

Note  $p$  is the number of voters.