University College London
Department of Computer Science

Reputable List Curation from Decentralized Voting

Elizabeth C. Crites*, Mary Maller, Sarah Meiklejohn, Rebekah Mercer

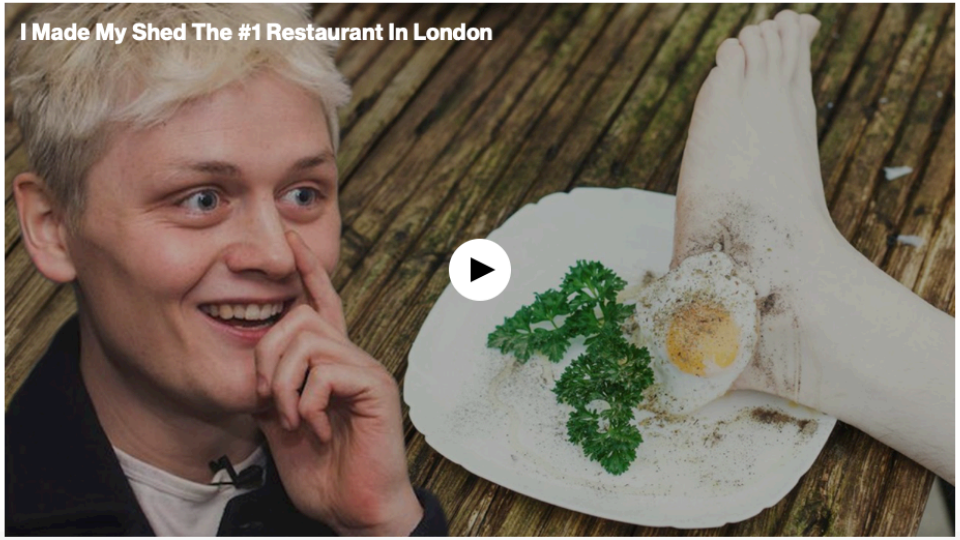
PETS - July 2020

I Made My Shed the Top-Rated Restaurant on TripAdvisor

And then served customers frozen dinners on its opening night.

OB By Oobah Butler

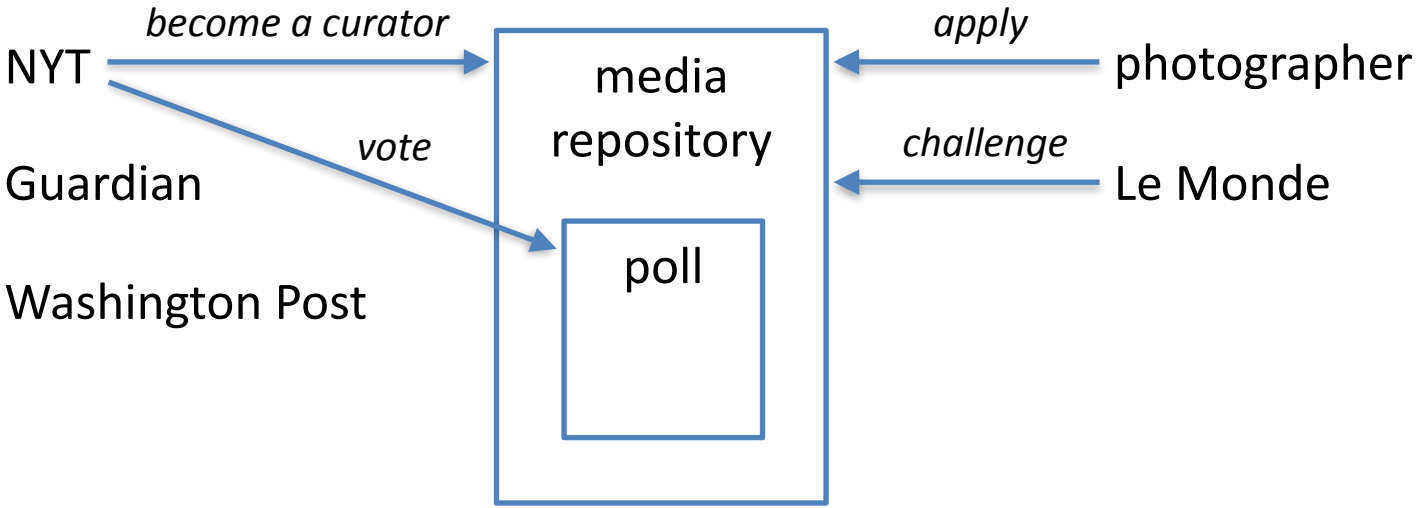
December 6, 2017, 12:20pm



The stunning hoax of The Shed at Dulwich deceived millions and showed how willing we are to consume an appetizing story. COURTESY VICE/THEO MCINNES

Applications:

1. Lists of good restaurants
2. New York Times News Provenance Project



Jerome Moore 1h ago

A tropical storm just hit the Florida coast! Stay safe!

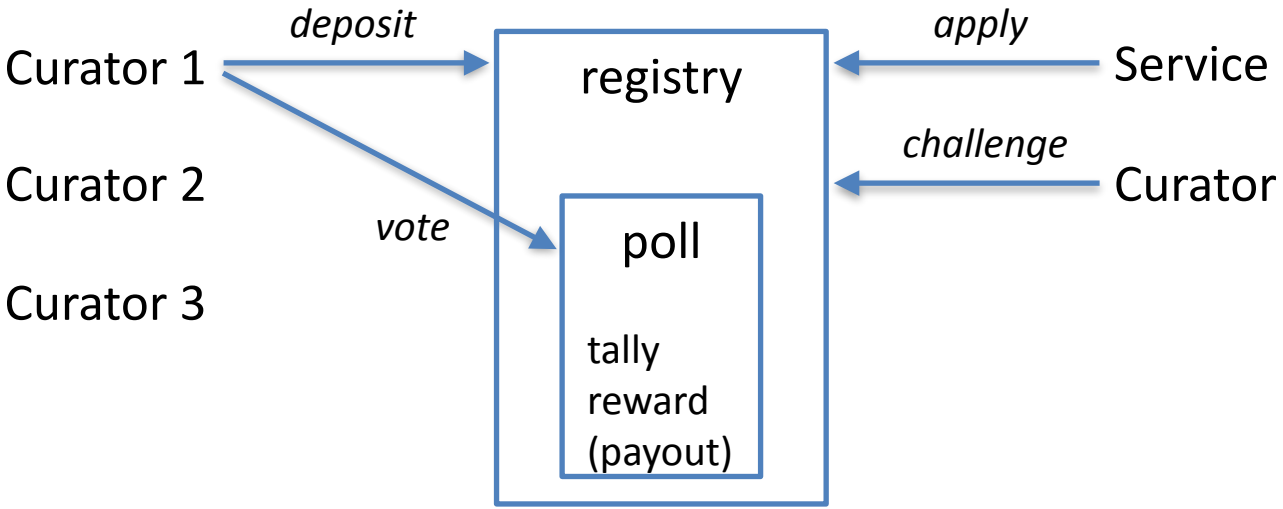
20 Likes 6 Comments Share

Image: NYT News Provenance Project www.newsprovenanceproject.com

Privacy:

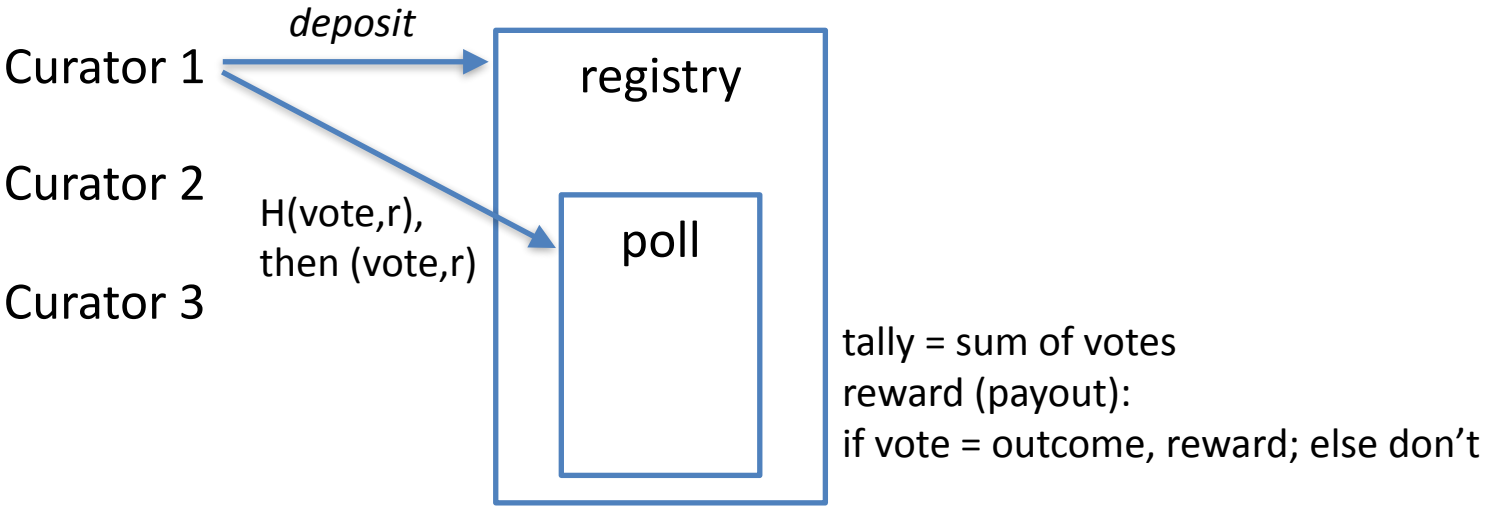
- business interests, social relationships, and potential conflicts of the participants can skew voting
- retaliation or bribery

Token-curated registry (TCR):



Existing solutions:

1. ConSensys Partial-Lock-Commit-Reveal reveals votes in the clear
2. Enigma relies on trusted hardware



Requirements for voting:

1. Vote Secrecy
    - votes are not revealed
2. Dispute Freeness
    - can verify if everyone is following the protocol
3. Self Tallying
    - tally can be computed by anyone

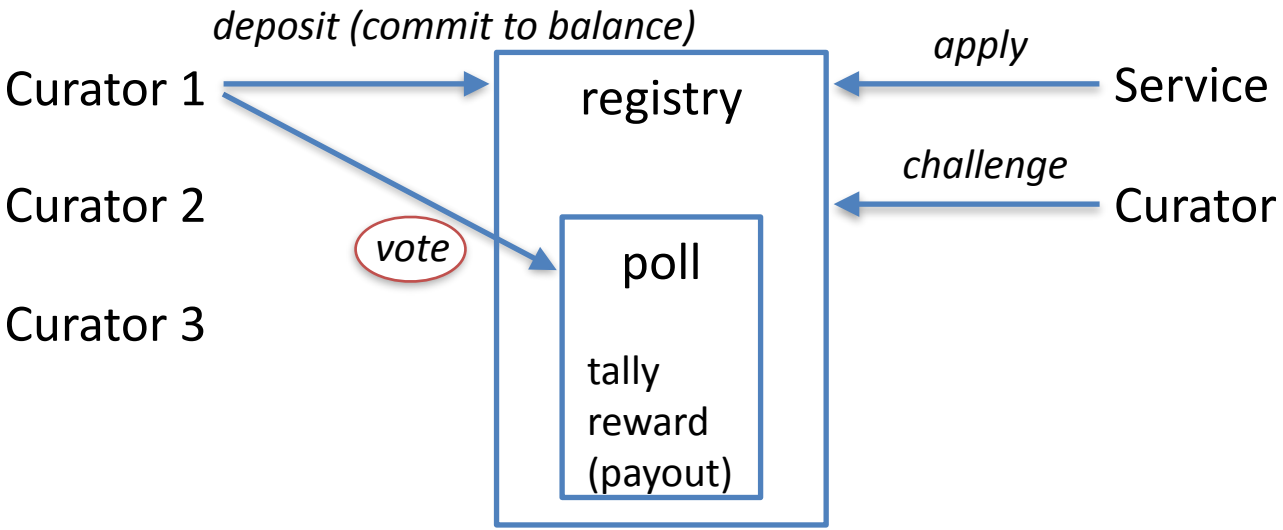
Our results:

1. Formal cryptographic model for TCRs

2. First provably secure construction of a TCR

3. Implementation as smart contract on Ethereum

Token-curated registry (TCR):



Voting protocol of [HRZ10]:

Registration :

$x \xleftarrow{\$} \mathbb{F}, c_0 \leftarrow g_0^x$

ZKP of x

Vote :

$$Y \leftarrow \prod_{0 \le i \le j, j < k \le m} c_{i,0} c_{k,0}^{-1}$$

$c_2 \leftarrow g_1^{\text{vote}} Y^x$

ZKP that vote $\in \{0,1\}$

implementation on Ethereum [MSH17]

Self tallying:

Voter 1

$$c_{1,0} = g_0^{x_1}$$

$$Y_1 = g_0^{-x_2} g_0^{-x_3}$$

$$Y_1^{x_1} = g_0^{x_1(-x_2-x_3)}$$

Voter 2

$$c_{2,0} = g_0^{x_2}$$

$$Y_2 = g_0^{x_1} g_0^{-x_3}$$

$$Y_2^{x_2} = g_0^{x_2(x_1-x_3)}$$

Voter 3

$$c_{3,0} = g_0^{x_3}$$

$$Y_3 = g_0^{x_1} g_0^{x_2}$$

$$Y_3^{x_3} = g_0^{x_3(x_1+x_2)}$$

find by brute force

$$\text{Tally} = \prod_{i=1}^{3} c_{i,2} = \prod_{i=1}^{3} g_1^{\text{vote}_i} Y_i^{x_i} = g_1^{\sum_{i=1}^{3} \text{vote}_i}$$

($Y_i^{x_i}$ struck through, with 1 above)

Requirements (Hao et al.):

1. Vote Secrecy 
   - votes are not revealed
2. Dispute Freeness 
   - can verify if everyone is following the protocol
3. Self Tallying 
   - tally can be computed by anyone

Our TCR construction:

register vote intention

Vote1 :

$$x \xleftarrow{\$} \mathbb{F}, (c_0, c_1) \leftarrow (g_0^x, g_1^{\text{vote}} h_0^x)$$

$$\pi_1 \leftarrow \text{Prove}(R_{\text{Vote1}}, c_0, x)$$

Vote2 :

$$Y \leftarrow \prod_{1 \le i \le j, j < k \le m} c_{i,0} c_{k,0}^{-1}$$

$$c_2 \leftarrow g_1^{\text{vote}} Y^x$$

$$\pi_2 \leftarrow \text{Prove}(R_{\text{Vote2}}, (Y, \{c_i\}_{i=0}^2), (\text{vote}, x))$$

Our TCR construction:

Deposit:

$C \leftarrow g_1^{\text{amt}} h_0^r$

Payout:

$c_1 \leftarrow g_1^{\text{vote}} h_0^x$

$b_1 = b_2$ arithmetized as $1 - b_1 - b_2 - 2b_1b_2$

For vote = outcome,

$g_1^{\text{amt}} h_0^r \cdot g_1^{1-\text{outcome}} g_1^{\text{vote}} h_0^{x(2\cdot\text{outcome}-1)}$

User can update commitment C:

	outcome = 0	outcome = 1
vote = 0	(amt + 1, $r - x$)	(amt, $r + x$)
vote = 1	(amt, $r - x$)	(amt + 1, $r + x$)

Results:

Theorem: If (Prove,Verify) is a zero-knowledge argument of knowledge and the decisional Diffie-Hellman (DDH) assumption holds, then our construction satisfies vote secrecy and dispute freeness.

1. Vote Secrecy ✓
2. Dispute Freeness ✓
3. Self Tallying ✓

Implementation on Ethereum:

- 256-bit primes & BN256 G1 curve

Stage	Time (μs)	Verification (gas)	Verification and tx (gas)	Verification and tx (USD)
Deposit	328	38,659	60,507	0.027
Update	328	18,641	40,489	0.018
Vote1	656	58,677	80,525	0.036
Vote2	3546	130,696	156,192	0.070
Total	4854	246,673	337,713	0.151

Future work:

- new proof techniques to make more efficient
- concurrency
  - new construction at eprint: 2020/709

Thank you!

contact: e.crites@ucl.ac.uk