Ring Signatures based anonymous voting

(Barreto-Naehrig 256 bit Elliplic Curve)

The goal

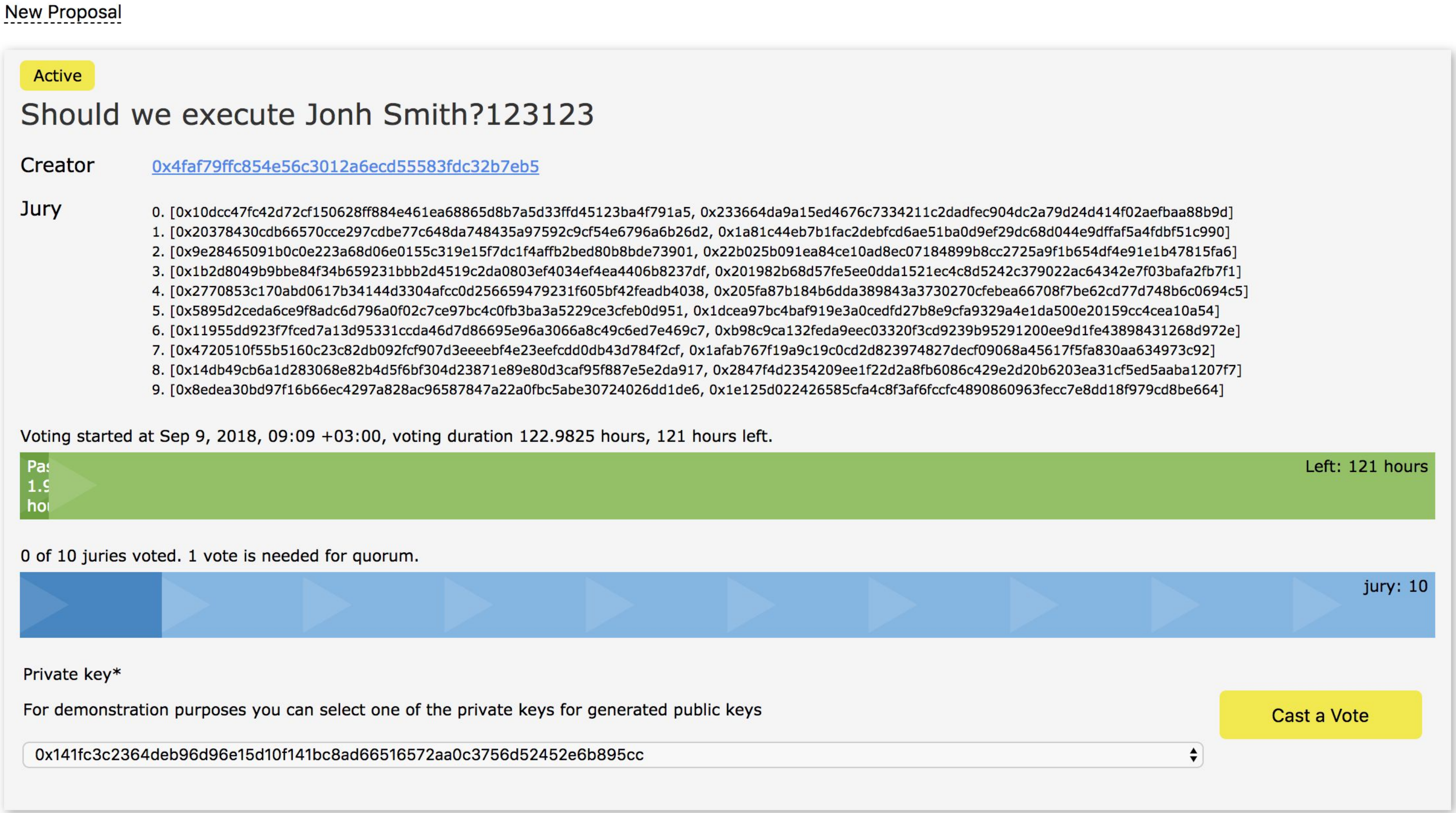
Create a cryptographically proofed anonymous method of decision making, especially relevant in sensitive spheres like life support, executions, mercy-killing etc.

Solution

On-chain anonymous voting based on Ring Signatures

How it works?

Overview



New Proposal

Active

Should we execute Jonh Smith?123123

Creator 0x4faf79ffc854e56c3012a6ecd55583fdc32b7eb5

Jury

0. [0x10dcc47fc42d72cf150628ff884e461ea68865d8b7a5d33ffd45123ba4f791a5, 0x233664da9a15ed4676c7334211c2dadfec904dc2a79d24d414f02aefbaa88b9d]
1. [0x20378430cdb66570cce297cdbe77c648da748435a97592c9cf54e6796a6b26d2, 0x1a81c44eb7b1fac2debfcd6ae51ba0d9ef29dc68d044e9dffaf5a4fdbf51c990]
2. [0x9e28465091b0c0e223a68d06e0155c319e15f7dc1f4affb2bed80b8bde73901, 0x22b025b091ea84ce10ad8ec07184899b8cc2725a9f1b654df4e91e1b47815fa6]
3. [0x1b2d8049b9bbe84f34b659231bbb2d4519c2da0803ef4034ef4ea4406b8237df, 0x201982b68d57fe5ee0dda1521ec4c8d5242c379022ac64342e7f03bafa2fb7f1]
4. [0x2770853c170abd0617b34144d3304afcc0d256659479231f605bf42feadb4038, 0x205fa87b184b6dda389843a3730270cfebea66708f7be62cd77d748b6c0694c5]
5. [0x5895d2ceda6ce9f8adc6d796a0f02c7ce97bc4c0fb3ba3a5229ce3cfeb0d951, 0x1dcea97bc4baf919e3a0cedfd27b8e9cfa9329a4e1da500e20159cc4cea10a54]
6. [0x11955dd923f7fced7a13d95331ccda46d7d86695e96a3066a8c49c6ed7e469c7, 0xb98c9ca132feda9eec03320f3cd9239b95291200ee9d1fe43898431268d972e]
7. [0x4720510f55b5160c23c82db092fcf907d3eeeebf4e23eefcdd0db43d784f2cf, 0x1afab767f19a9c19c0cd2d823974827decf09068a45617f5fa830aa634973c92]
8. [0x14db49cb6a1d283068e82b4d5f6bf304d23871e89e80d3caf95f887e5e2da917, 0x2847f4d2354209ee1f22d2a8fb6086c429e2d20b6203ea31cf5ed5aaba1207f7]
9. [0x8edea30bd97f16b66ec4297a828ac96587847a22a0fbc5abe30724026dd1de6, 0x1e125d022426585cfa4c8f3af6fccfc4890860963fecc7e8dd18f979cd8be664]

Voting started at Sep 9, 2018, 09:09 +03:00, voting duration 122.9825 hours, 121 hours left.

0 of 10 juries voted. 1 vote is needed for quorum.

Private key*

For demonstration purposes you can select one of the private keys for generated public keys

0x141fc3c2364deb96d96e15d10f141bc8ad66516572aa0c3756d52452e6b895cc

1. Creation of voting

Judge:

— Creates a voting on some topic, f.e. "Death sentence hearing on case #01232".

— Publishes N public keys of juries and sets quorum number M: M <= N — amount of needed votes "for".

— Sets voting deadline.

2. Voting process

Each jury:
— Generates message, voting "for" judge's decision. Voting "against" is passive (just do nothing).

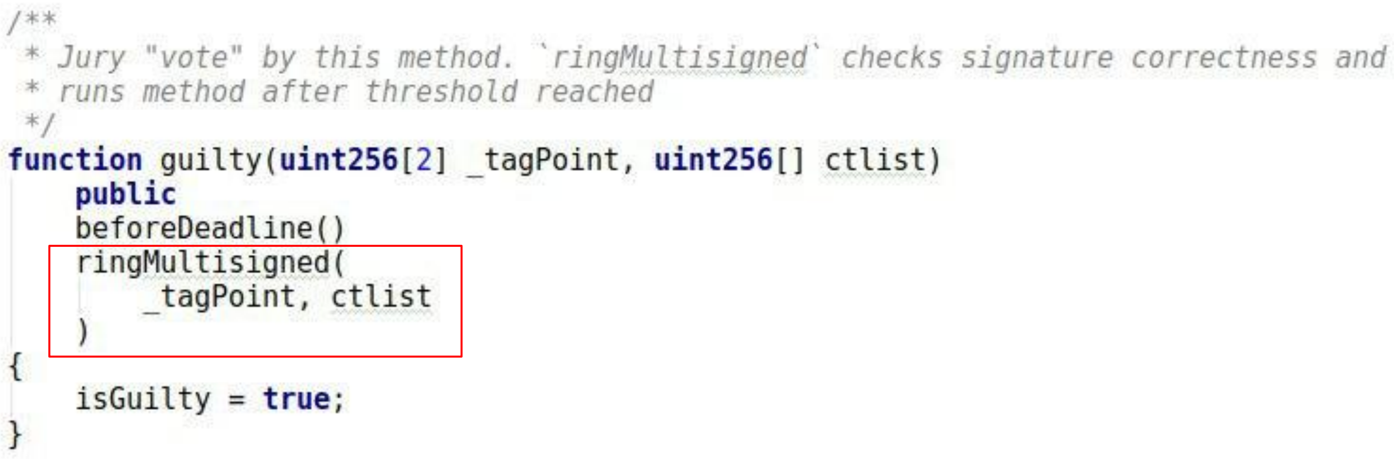
— Generates ring-signature for this message, using public keys of other juries (under the hood).

— Sends transaction with ring-signature to contract.

3. Decision

If M of N votes "for"
is reached,
action is performed.

The Library



```
/**
 * Jury "vote" by this method. `ringMultisigned` checks signature correctness and
 * runs method after threshold reached
 */
function guilty(uint256[2] _tagPoint, uint256[] ctlist)
    public
    beforeDeadline()
    ringMultisigned(
        _tagPoint, ctlist
    )
{
    isGuilty = true;
}
```

We’ve implemented the library for protecting any function of any contract with anonymous ring multisignature.