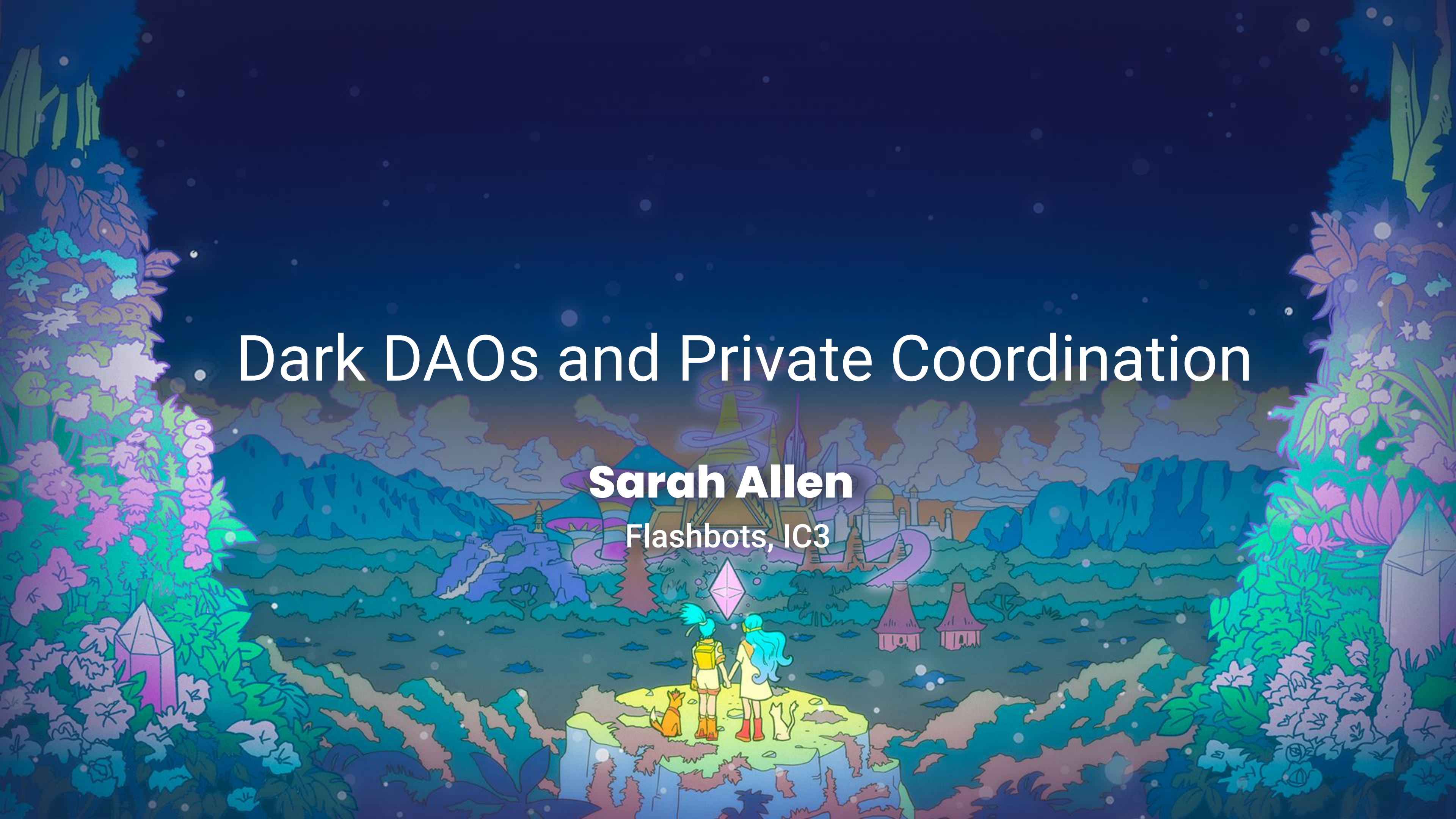


Dark DAOs and Private Coordination

Sarah Allen

Flashbots, IC3

Assumptions About Private Keys

- Must be kept secret to be secure
- Assumed to be held by one person (or entity)
- Any signature is assumed to be created by the owner
- Anything singed is assumed to be signed with the owner’s consent

Assumption: private keys are exclusively held and used by their owner

Private Key = Identity

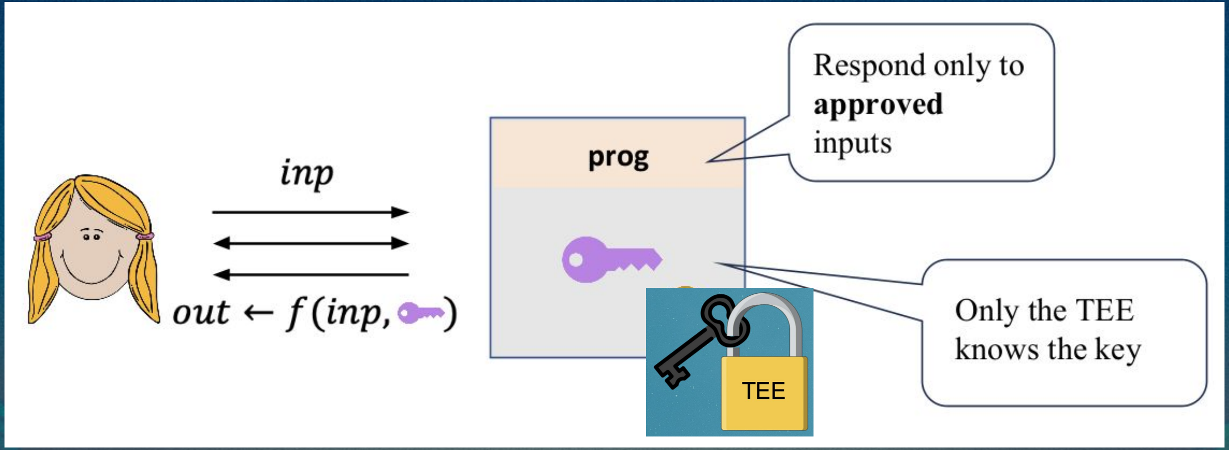
What if an owner could share or rent the right to sign with their key?

~~Private Key = Identity~~

+ Encumbrance

Encumbrance

- A secret key can be generated in a trusted execution environment (TEE)
- The key then continues to live in the TEE
- The TEE can be used to apply complex policies to the use of that private key



Respond only to **approved** inputs

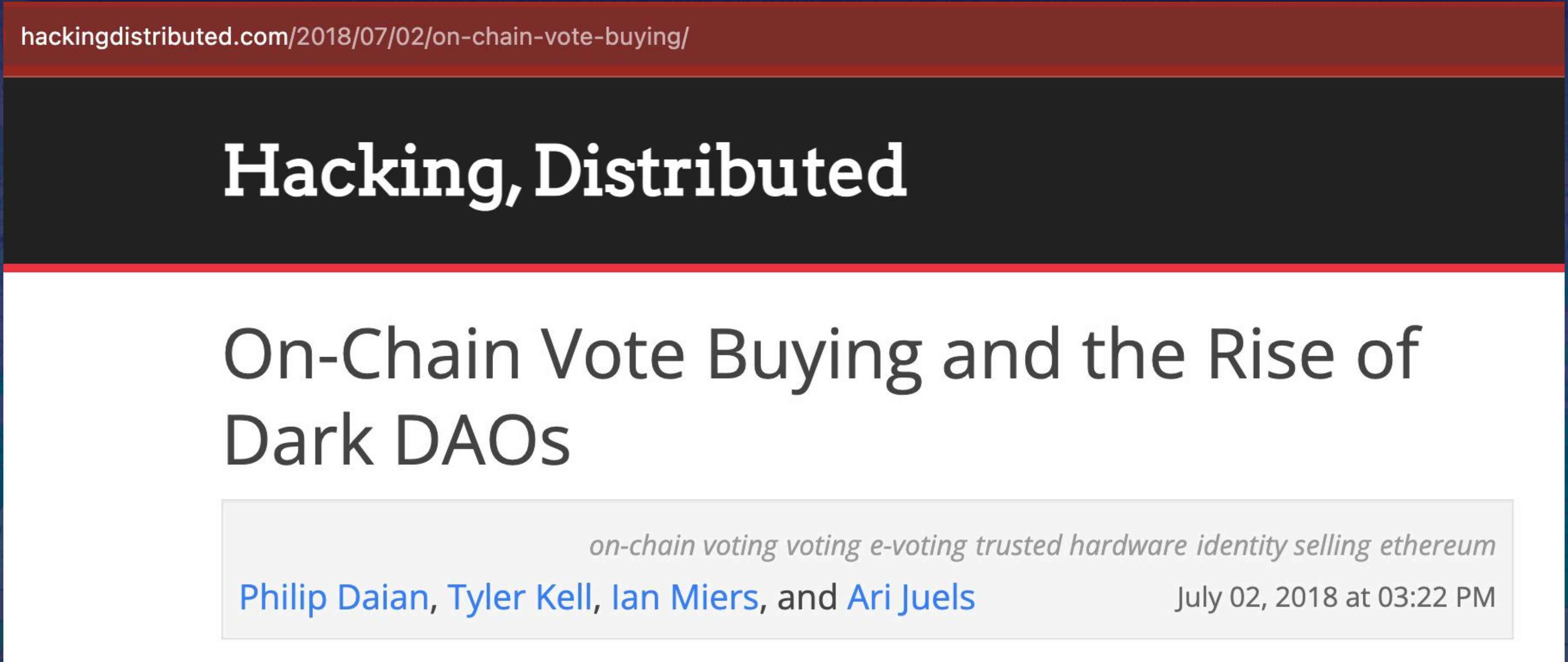
Only the TEE knows the key

Private Keys Assumptions in the Presence of TEEs

- Must be kept secret to be secure
- ~~Assumed to be held by one person (or entity)~~
- ~~Any signature is assumed to be created by the owner~~
- ~~Anything singed is signed with the owner’s consent~~

The single-entity address-ownership (SEAO) assumption is broken by encumbrance.

This has wide ranging implications.



hackingdistributed.com/2018/07/02/on-chain-vote-buying/

Hacking, Distributed

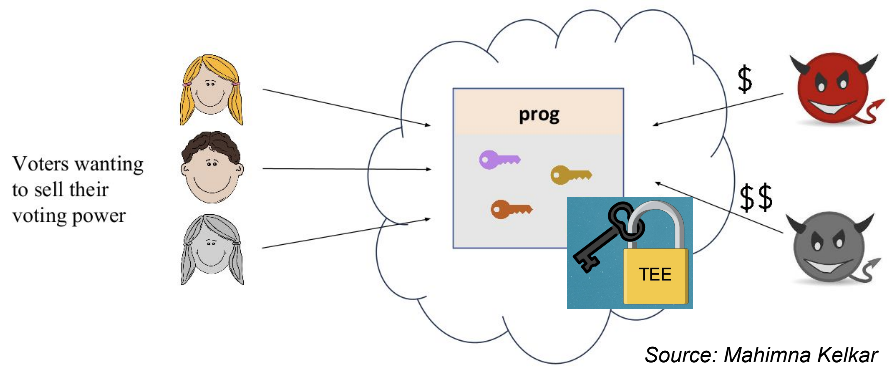
On-Chain Vote Buying and the Rise of Dark DAOs

on-chain voting voting e-voting trusted hardware identity selling ethereum

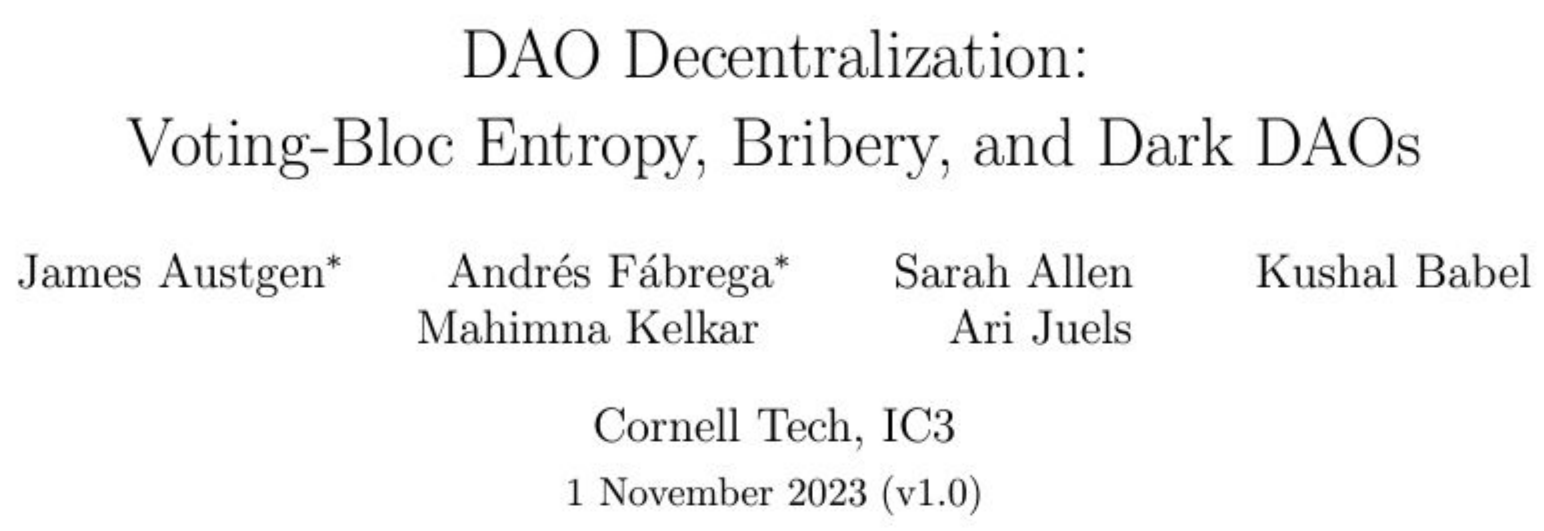
Philip Daian, Tyler Kell, Ian Miers, and Ari Juels July 02, 2018 at 03:22 PM

Dark DAO

- “A Dark DAO is a decentralized cartel that buys on-chain votes opaquely (“in the dark”).”
- Potentially nobody (not even the creator) can determine:
    - The total number of participants
    - The total amount pledged
    - The precise logic of the Dark DAO



Source: Mahimna Kelkar

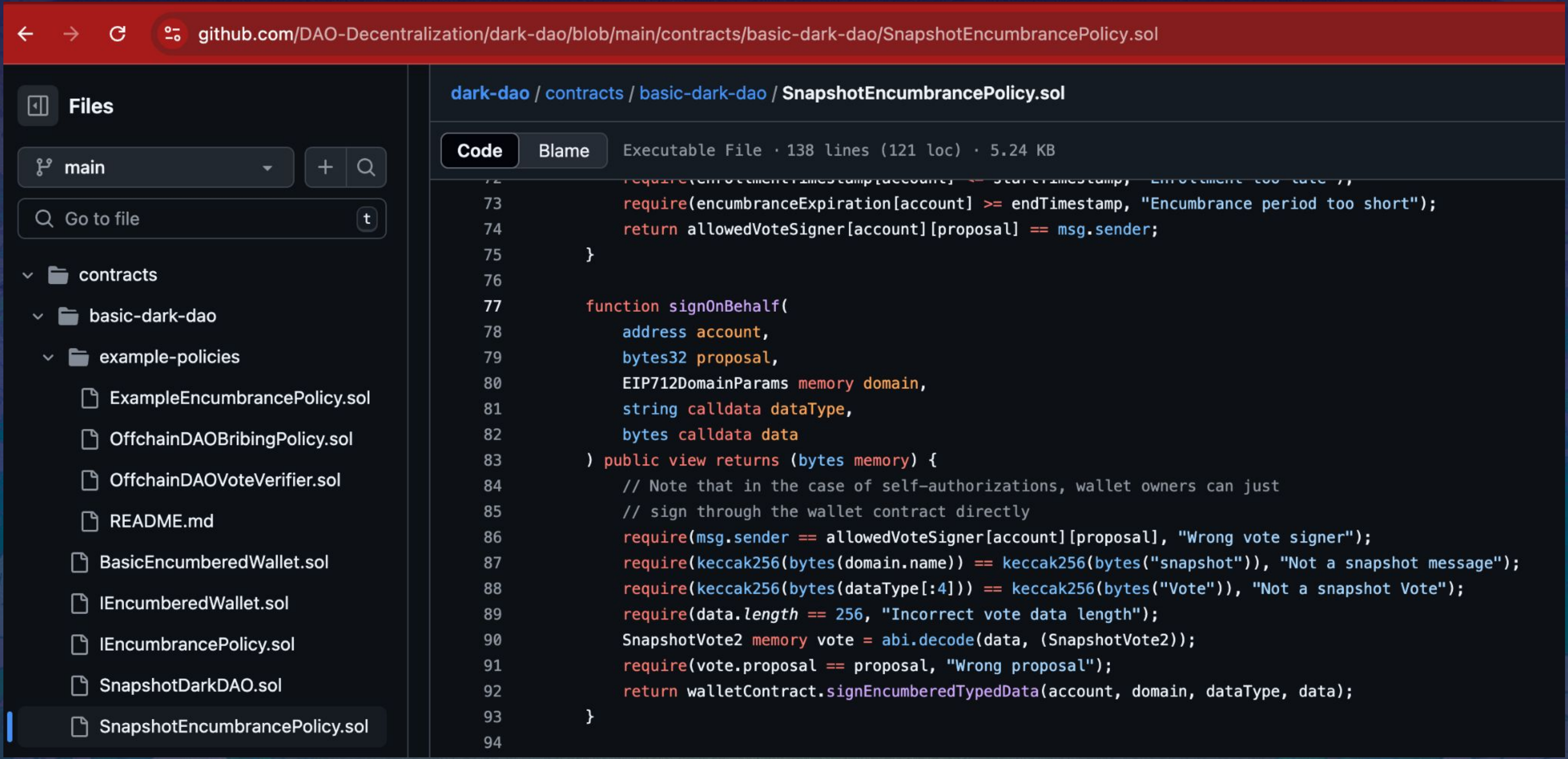


DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs

James Austgen* Andrés Fábrega* Sarah Allen Kushal Babel
Mahimna Kelkar Ari Juels

Cornell Tech, IC3

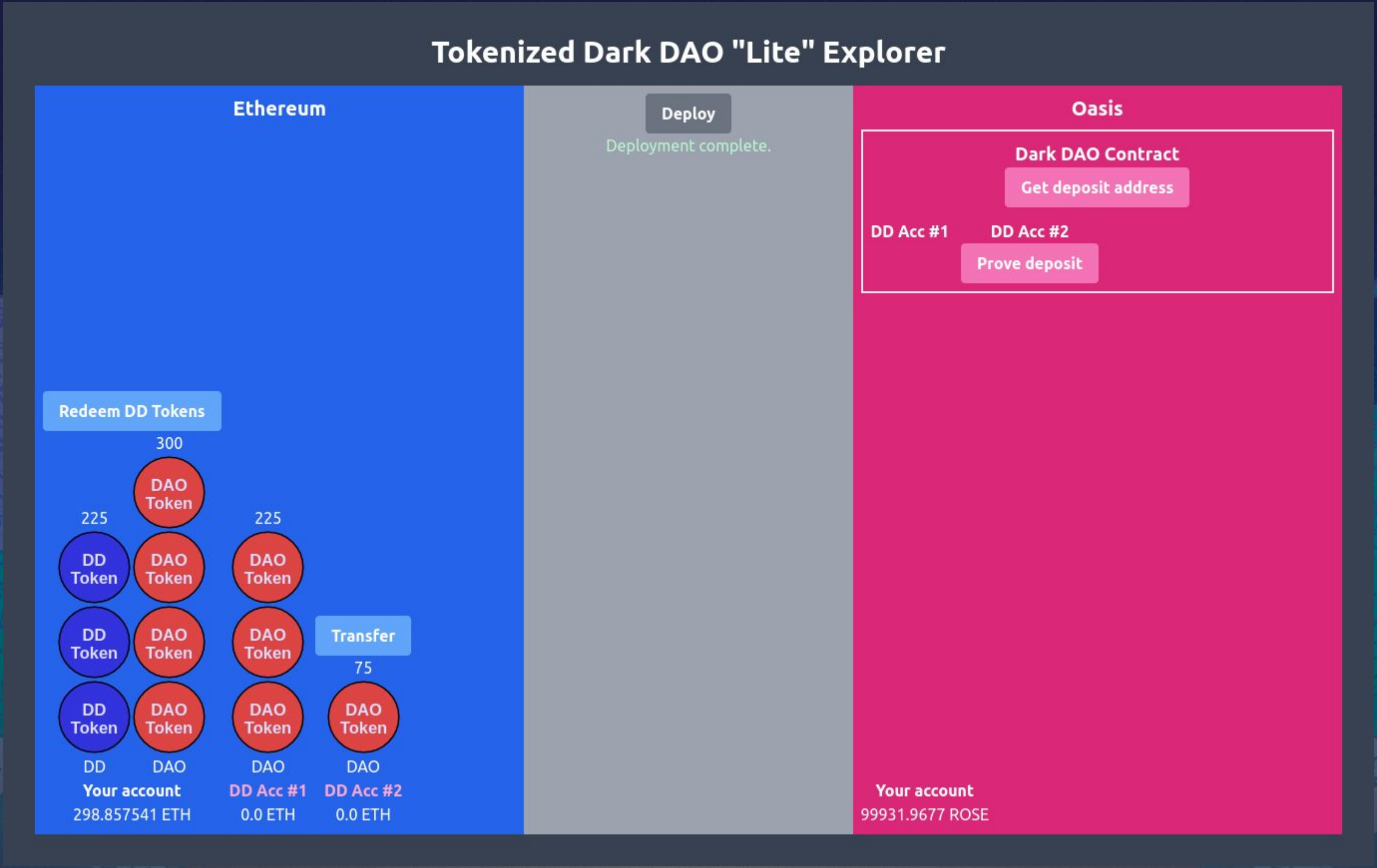
1 November 2023 (v1.0)


github.com/DAO-Decentralization/dark-dao/blob/main/contracts/basic-dark-dao/SnapshotEncumbrancePolicy.sol
Files
main
Go to file
t
contracts
basic-dark-dao
example-policies
ExampleEncumbrancePolicy.sol
OffchainDAOBribingPolicy.sol
OffchainDAOVoteVerifier.sol
README.md
BasicEncumberedWallet.sol
IEncumberedWallet.sol
IEncumbrancePolicy.sol
SnapshotDarkDAO.sol
SnapshotEncumbrancePolicy.sol
dark-dao / contracts / basic-dark-dao / SnapshotEncumbrancePolicy.sol
Code
Blame
Executable File · 138 lines (121 loc) · 5.24 KB

```
        require(enrollmentTimestamp[account] <= startTimestamp, "Enrollment too late");
        require(encumbranceExpiration[account] >= endTimestamp, "Encumbrance period too short");
        return allowedVoteSigner[account][proposal] == msg.sender;
    }

    function signOnBehalf(
        address account,
        bytes32 proposal,
        EIP712DomainParams memory domain,
        string calldata dataType,
        bytes calldata data
    ) public view returns (bytes memory) {
        // Note that in the case of self-authorizations, wallet owners can just
        // sign through the wallet contract directly
        require(msg.sender == allowedVoteSigner[account][proposal], "Wrong vote signer");
        require(keccak256(bytes(domain.name)) == keccak256(bytes("snapshot")), "Not a snapshot message");
        require(keccak256(bytes(dataType[:4])) == keccak256(bytes("Vote")), "Not a snapshot Vote");
        require(data.length == 256, "Incorrect vote data length");
        SnapshotVote2 memory vote = abi.decode(data, (SnapshotVote2));
        require(vote.proposal == proposal, "Wrong proposal");
        return walletContract.signEncumberedTypedData(account, domain, dataType, data);
    }

```



Tokenized Dark DAO "Lite" Explorer

Deployment complete.

Your account
298.857541 ETH

DD Acc #1
0.0 ETH

DD Acc #2
0.0 ETH

Your account
99931.9677 ROSE

Liquefaction

Liquefaction

- An encumbered wallet platform
- Allows users to attach rich, multi-user policies to accounts
- Enables the credentials and assets of a single end-user address to be freely rented, shared, or pooled
- Accomplishes these things privately with no direct on-chain traces

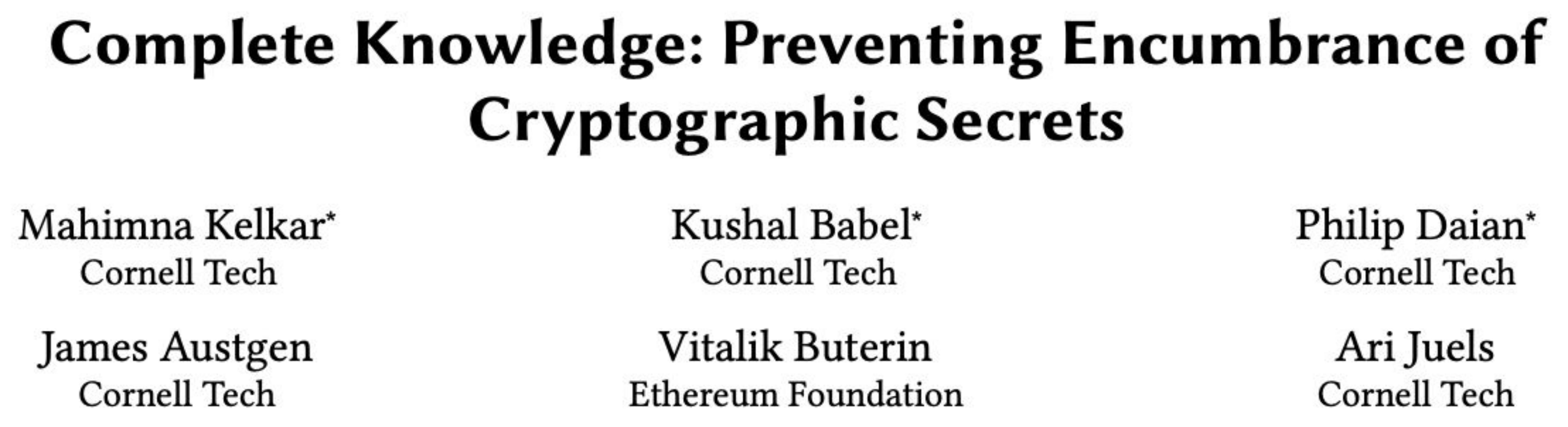
Broadly, it enables the transfer of things thought to be non-transferable

What is Impacted by Liquefaction?

- Private DAOs
- Quadratic voting and quadratic funding
- Soulbound tokens
- Rights to airdrops and activity-based rewards
- Dusting attacks
- Locked tokens
- Onchain/offchain transacting
- Multisigs
- Allow lists

See more in the upcoming Liquefaction paper

What can you do in settings where you do not want undetected encumbrance?



Complete Knowledge: Preventing Encumbrance of Cryptographic Secrets

Mahimna Kelkar*
Cornell Tech

Kushal Babel*
Cornell Tech

Philip Daian*
Cornell Tech

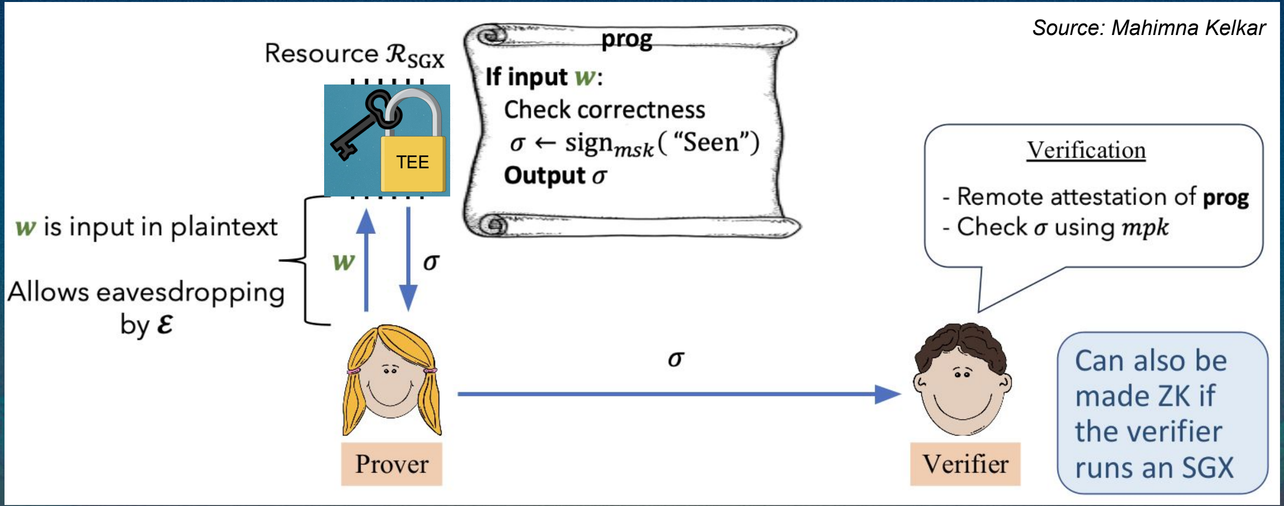
James Austgen
Cornell Tech

Vitalik Buterin
Ethereum Foundation

Ari Juels
Cornell Tech

How CK Works

- A Proof of Complete Knowledge (CK) shows fully unencumbered knowledge of a secret
- It does this by proving that the key has been leaked over an insecure channel
- Can be done with a TEE or ASIC



Source: Mahimna Kelkar

w is input in plaintext

Allows eavesdropping by $\mathcal{E}$

prog

```
If input $w$:
    Check correctness
    $\sigma \leftarrow \text{sign}_{msk}(\text{"Seen"})$
    Output $\sigma$
```

Verification

- Remote attestation of **prog**
- Check σ using mpk

Can also be made ZK if the verifier runs an SGX

Where is this taking us?

State of Encumbrance

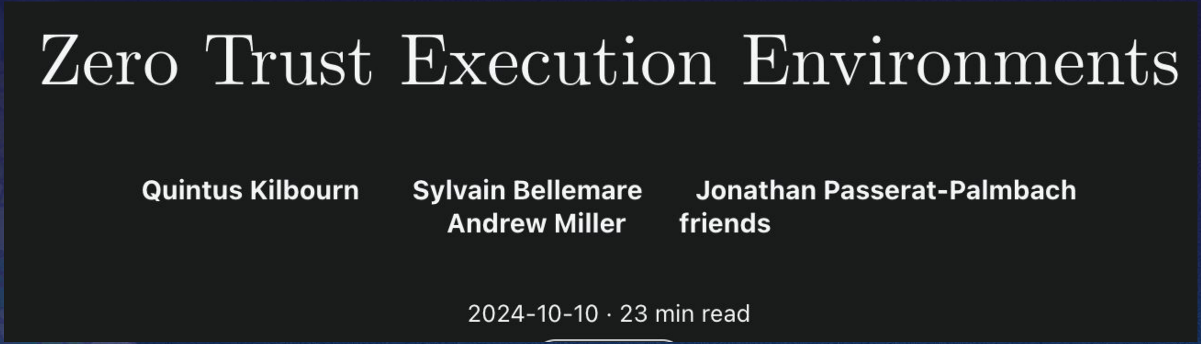
- Encumbrance in TEEs breaks assumptions underlying blockchain systems
- Additional measures (like CK) must be added in systems that want to ensure signer = account owner = a single individual/entity
- The most practical implementation of CK relies on TEEs

Undetectable encumbrance is already practical.

The defense against undetectable encumbrance will likely rely on TEEs.

What’s Next

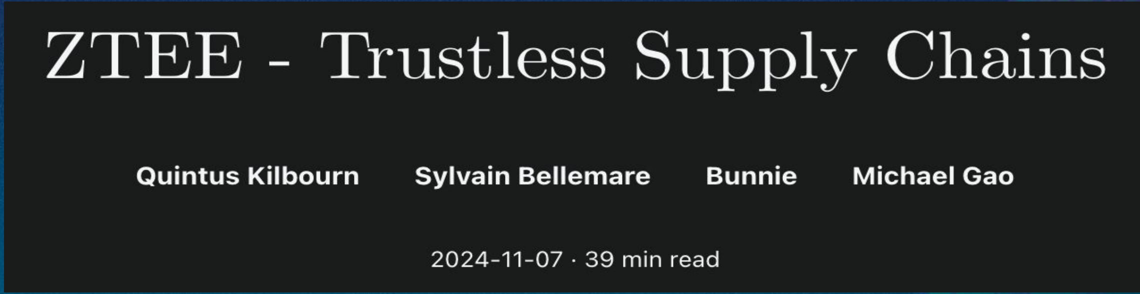
- Crowdsource a more complete list of systems that rely on assumptions broken by encumbrance
- Spread awareness that signer may /= account owner in current systems; design to either accept or take measures against this
- For those wishing to take measures against this, adopt CK
- Focus community effort on deep research on TEEs to develop an open TEE for our open systems



Zero Trust Execution Environments

Quintus Kilbourn   Sylvain Bellemare   Jonathan Passerat-Palmbach
Andrew Miller   friends

2024-10-10 · 23 min read



ZTEE - Trustless Supply Chains

Quintus Kilbourn   Sylvain Bellemare   Bunnie   Michael Gao

2024-11-07 · 39 min read

Check out the materials from TEE.salon
Find these post at writings.flashbots.net
Follow project TTEE and get involved on https://collective.flashbots.net

Resource List

- On-Chain Vote Buying and the Rise of Dark DAOs (11)
- DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs (13)
- DAO Decentralization and Dark DAO Github repository (14, 15)
- Dark DAO Lite demo (15)
- DAOs Must Confront Dark DAOs — Or Fall Under Their Shadow (13, 14, 15)
- Liquefaction paper (coming soon)
- Liquefaction Github repository (coming soon)
- Complete Knowledge: Preventing Encumbrance of Cryptographic Secrets (20)
- Zero Trust Execution Environments (26)
- ZTEE - Trustless Supply Chains (26)

I will share these slides on https://x.com/sarahalle_ (@sarahalle_)

Thank you!