# Censorship Resistance
# of
# Permissioned Ledgers

# Survivability Analysis

Phil Windley Ph.D. and Samuel M. Smith Ph.D.
IIW Fall 2019 2019/10/01
phil@windley.org sam@samuelsmith.org
https://github.com/SmithSamuelM/Papers

# Mission Survivability

Achieve Mission objectives despite adversary

Susceptibility:  Likelihood of being targeted for attack

Vulnerability: Likelihood of attack succeeding once targeted

Recoverability: Likelihood of repairing a successful attack

# *Dwitter* Censorship Resistance Example

- Activist using SSI on decentralized version of Twitter called *Dwitter*.
- Mission is to *credibly* protest government action.
- The activist has a public identifier, anchored in a blockchain distributed ledger.
- The activist is identified in this case by the identifier and associated attributes.
- The identifier is bound to a cryptographically-secure public/private key pair.
- Because the activist is the only one with access to the private key, only the activist can use it to create verifiably non-repudiable assertions sourced from that identifier.

# D*witter* Censorship Resistance Example

- In a permissioned ledger, because the validator nodes are known, the government could mount a censorship attack against the validator nodes within its jurisdiction and thereby force them to reduce the ability of the activist to use Dwitter to protest government action.
- In a permissionless ledger the validator nodes are many and diverse and the government is much less able to mount a censorship attack
- It would seem therefore that a permission-less ledger is essential to ensure the activist's is able to credibly protest government action.

# Caveats

*content anchor* = data item reference that includes a cryptographic signature of the associated content data.

*successful protest* = new supporters are able to discover content via content anchors on the public ledger and then verify the content as sourced from the activist.

identifier (public key) used to verify content/content anchor is pseudonymous

new supporters may only discover content anchors via ledger

# Attacks

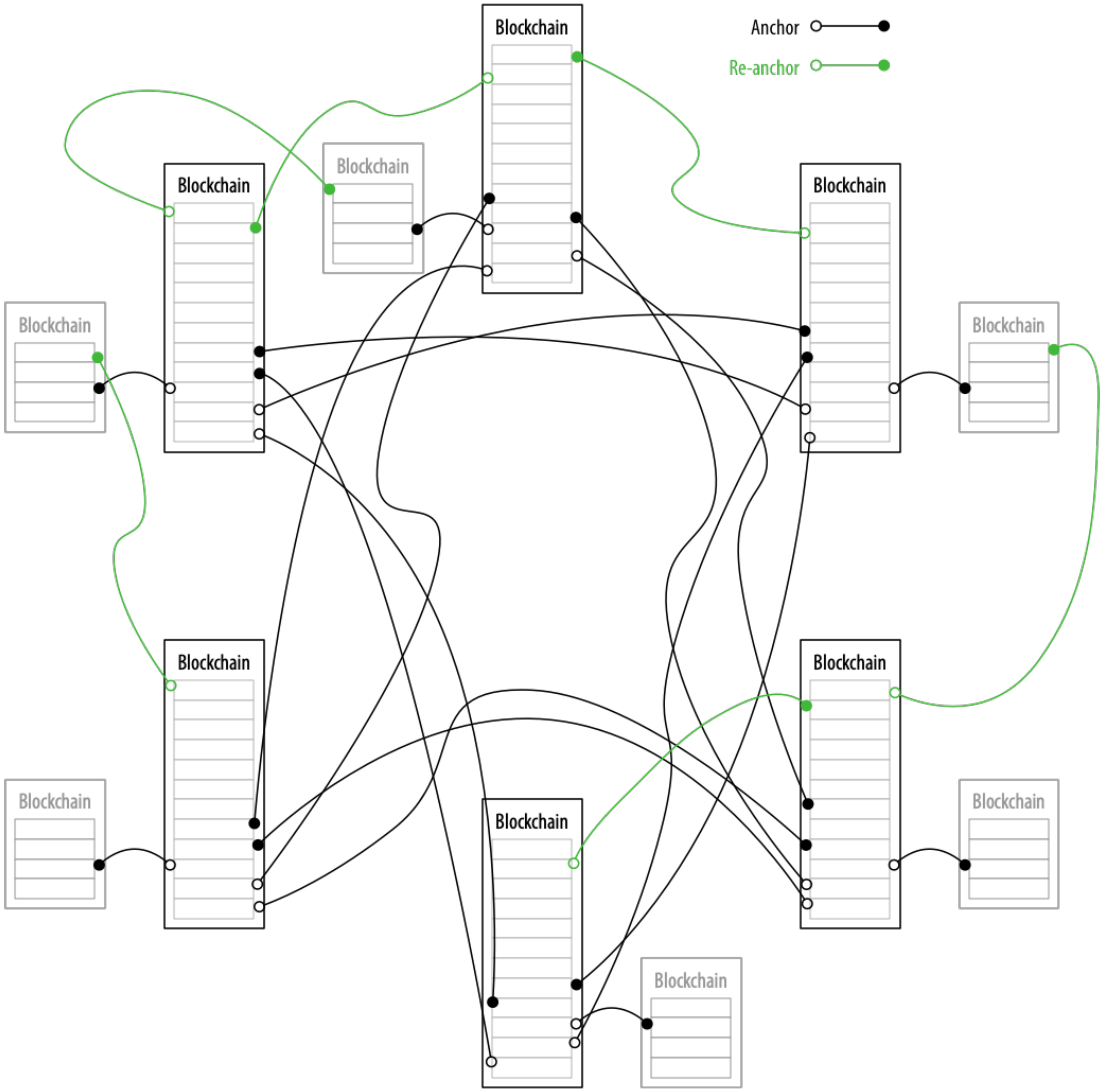
1. block the activist’s ability to request writes of content anchors to the ledger

2.  block the ability of others to verify ledger anchored content written by the activist

3. delete all the activist’s associated content anchors stored on the ledger

4. disrupt the operation of the ledger (prevent consensus)

# Mesh Anchoring



Blockchain
Anchor
Re-anchor
Blockchain
Blockchain
Blockchain
Blockchain
Blockchain
Blockchain
Blockchain
Blockchain
Blockchain
Blockchain
Blockchain
Blockchain