



Plural Publics

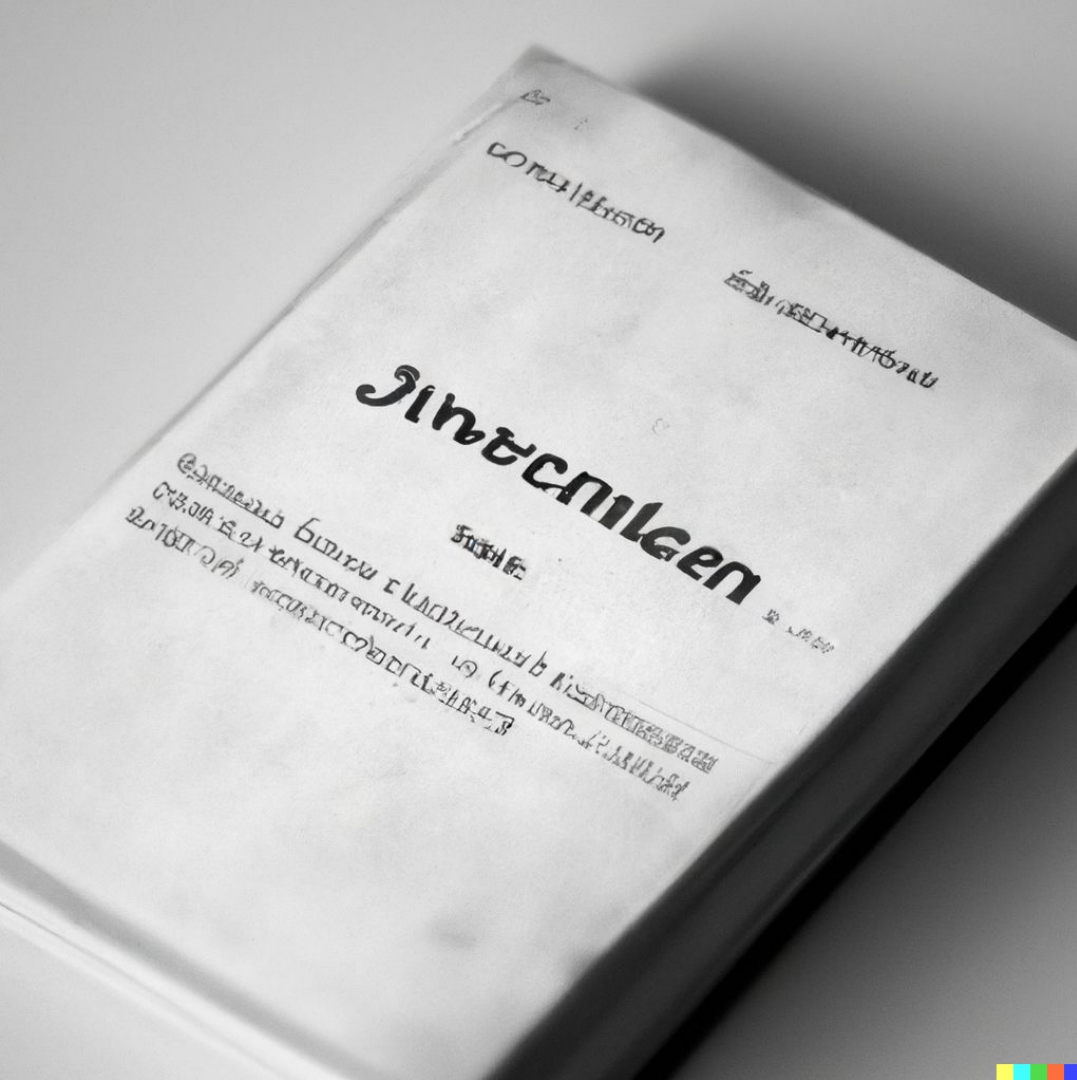
cooperation across social difference

Shrey Jain

Web3 Researcher, Microsoft

All images in this talk are
generated by DALLÉ-2.





Unique Dictionaries



A Riff on The Source Code Theorem





A Riff on The Source Code Theorem

Cultural communities minimize the number of bits needed to communicate within the group.





Speaking the language does NOT
mean you are “in” the group.



3 Scientists on a Panel



3 Scientists on a Panel

We are unable to preserve richness of communication during translation across differences today.



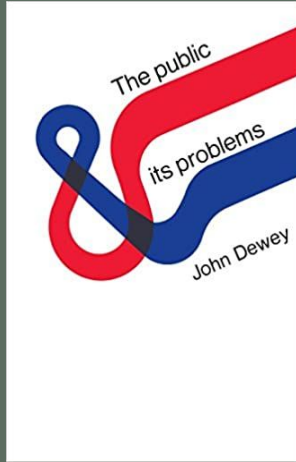
Plural Publics

Shrey Jain

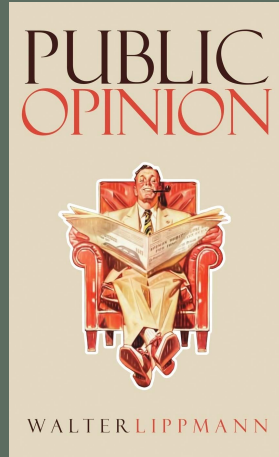
Web3 Research, Microsoft

Joint work with Glen Weyl, Yorke Rhodes, and Divya Siddarth

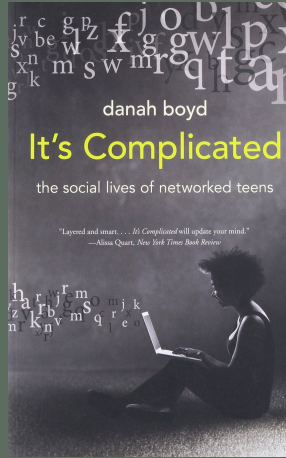




John Dewey



Walter Lippmann



danah boyd



Joseph Halpern

Cooperation

across

social differences

Cooperation

across

social differences

Common Knowledge





Common Knowledge

Everyone knows that ϕ is true,

Everyone knows that everyone knows that ϕ is true,

Everyone knows that everyone knows that
everyone knows that ϕ is true.

and so on, ad infinitum.



Coordinated Attack Problem



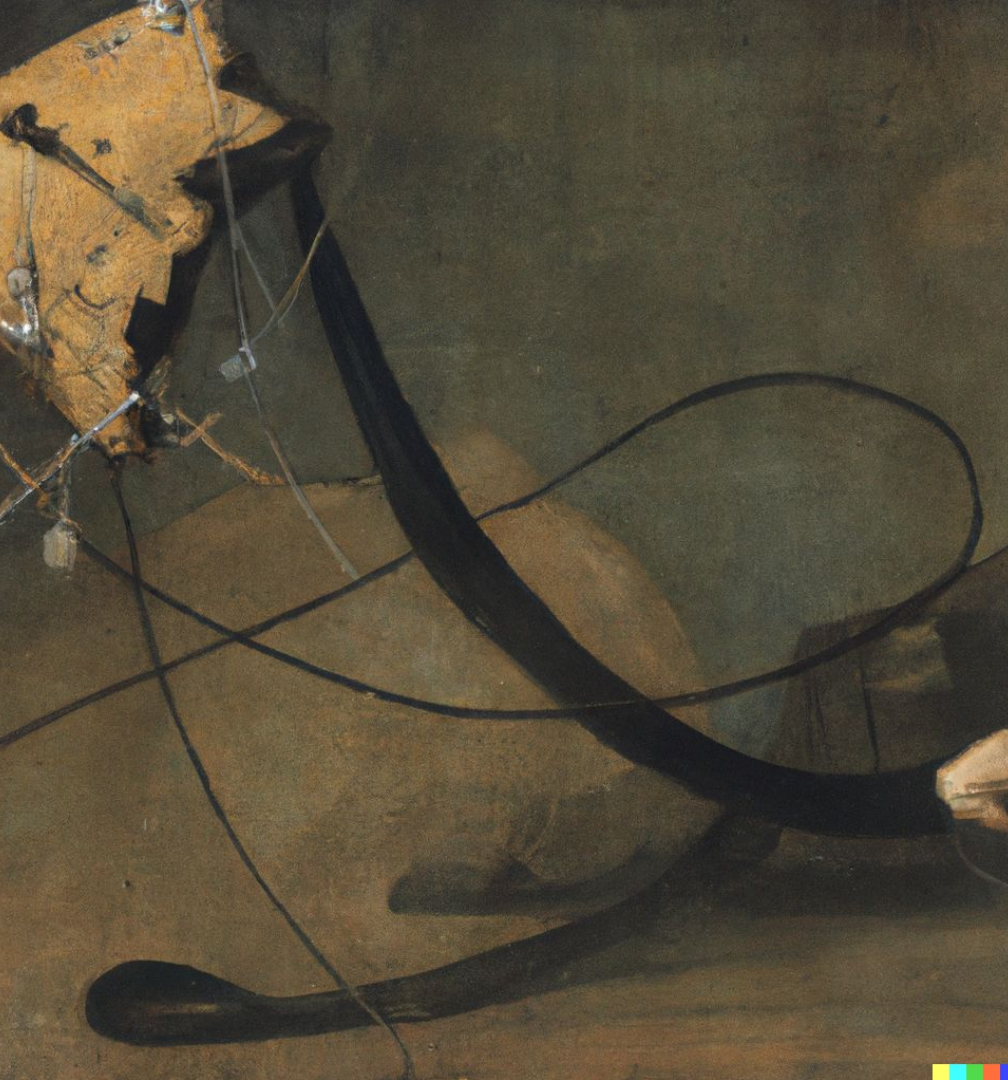
Coordinated Attack Problem



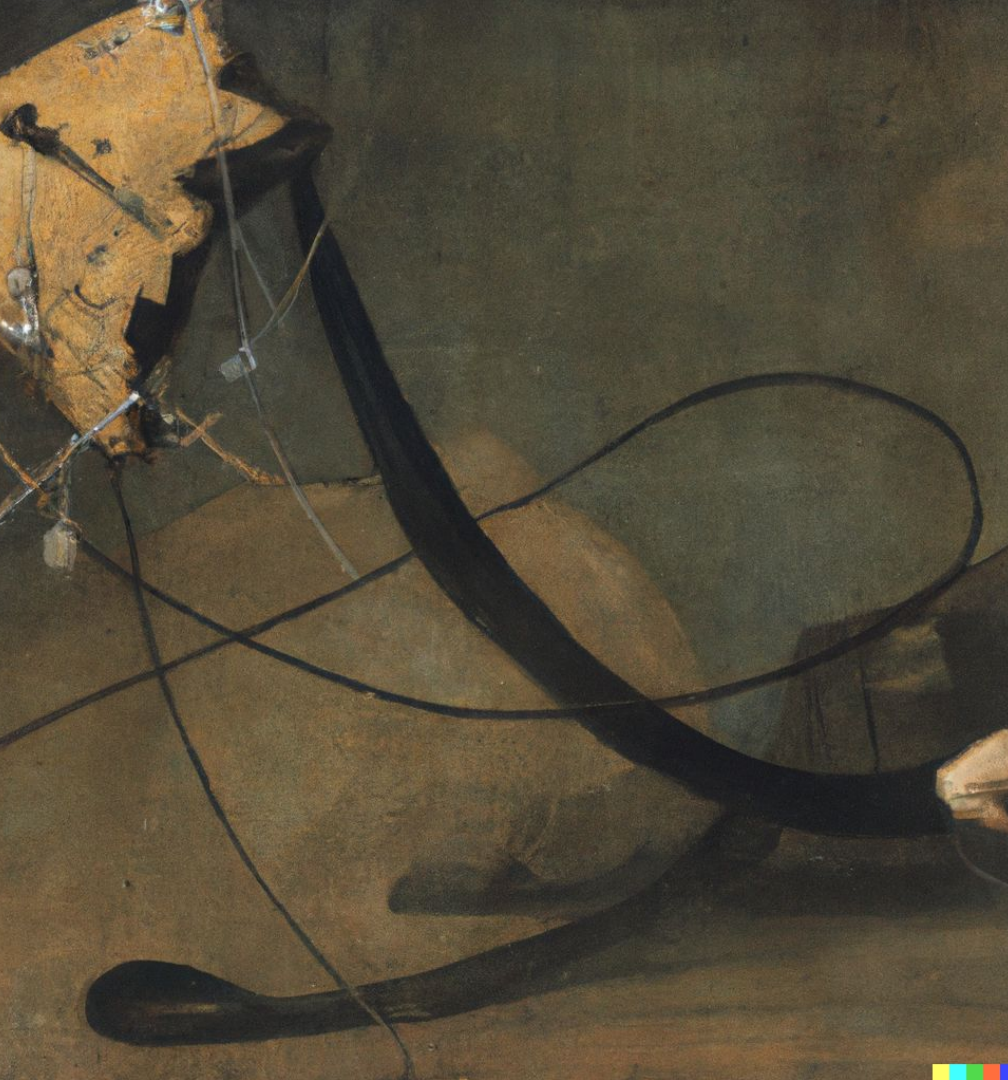
Coordinated Attack Problem



Coordinated Attack Problem



Common knowledge is not
attainable in systems where
communication is not
guaranteed.



Common knowledge is not
attainable in systems where
communication is not
guaranteed.

Aim to attain strong forms of
common-p belief.



Coordination

A set of agents take action simultaneously.



Coordination

A set of agents take action simultaneously.

Cooperation

A set of agents take action simultaneously and understand the payoffs that come with actions taken.

Cooperation

Altruism

Mutualism

Cooperation

Altruism: a cooperator confers a benefit at a cost to themselves

- Challenge to psychologists is how humans surmount this cost
- Measuring a suite of emotions like trust, empath, anger, etc.

Mutualism

Cooperation

Altruism: a cooperator confers a benefit at a cost to themselves

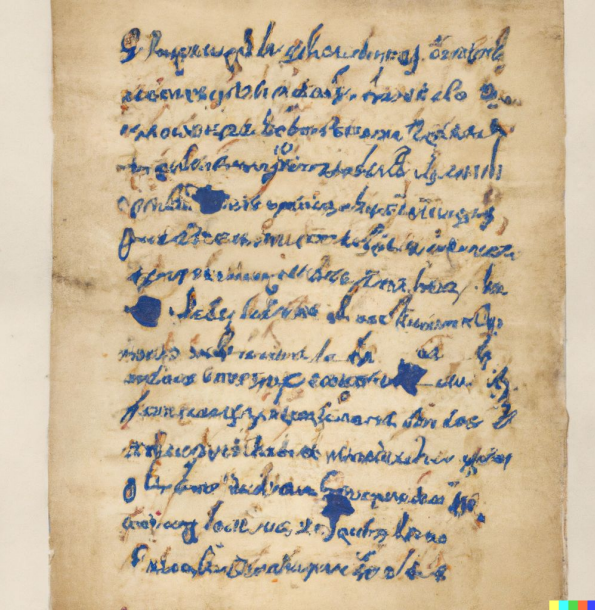
- Challenge to psychologists is how humans surmount this cost
- Measuring a suite of emotions like trust, empath, anger, etc.

Mutualism: each cooperator confers a benefit on the other while simultaneously conferring a benefit on themselves

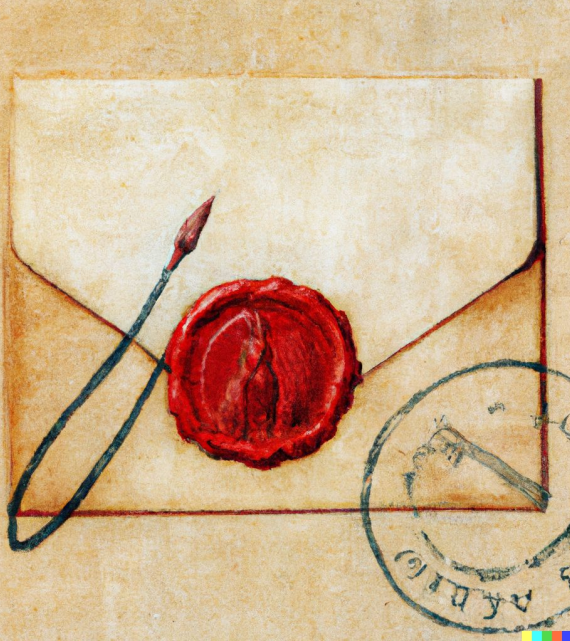
- Purely an **epistemological** challenge: measuring the knowledge someone else has
- Humans can categorize when someone has common knowledge
- Probability of action is significantly higher when common knowledge is attained



	Common p-belief	Privacy
Oral	Weak	Assume no leakage



	Common p-belief	Privacy
Oral	Weak	Assume no leakage
Writing	Weak Full message is sent	Assume no leakage



	Common p-belief	Privacy
Oral	Weak	Assume no leakage
Writing	Weak Full message is sent	Assume no leakage
Envelopes	Weak Full message is sent	Mitigates leakage



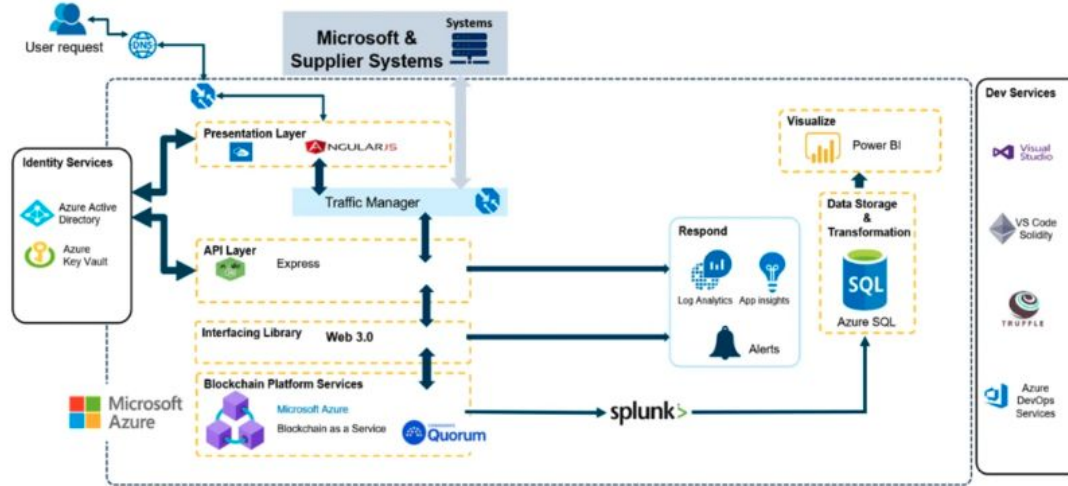
	Common p-belief	Privacy
Oral	Weak	Assume no leakage
Writing	Weak Full message is sent	Assume no leakage
Envelopes	Weak Full message is sent	Mitigates leakage
...		
SMTP, SMS, XMPP	Stronger but not sufficient	Mitigates leakage



DLTs are the next step in the progress of communication

1. DLTs have an easier interface to attain common-p belief
2. DLTs and blockchains enable us to provide **commitment**

Architecture Components



Save \$50 M/y in supply chain using a blockchain to communicate

We lack a commitment to knowledge.

Cooperation

across

social differences

Recognition

A Plural Decentralized Identity Frontier: Abstraction v. Composability Tradeoffs in Web3*

Shrey Jain[†]

University of Toronto
shreyjaineth@gmail.com

Leon Erichsen

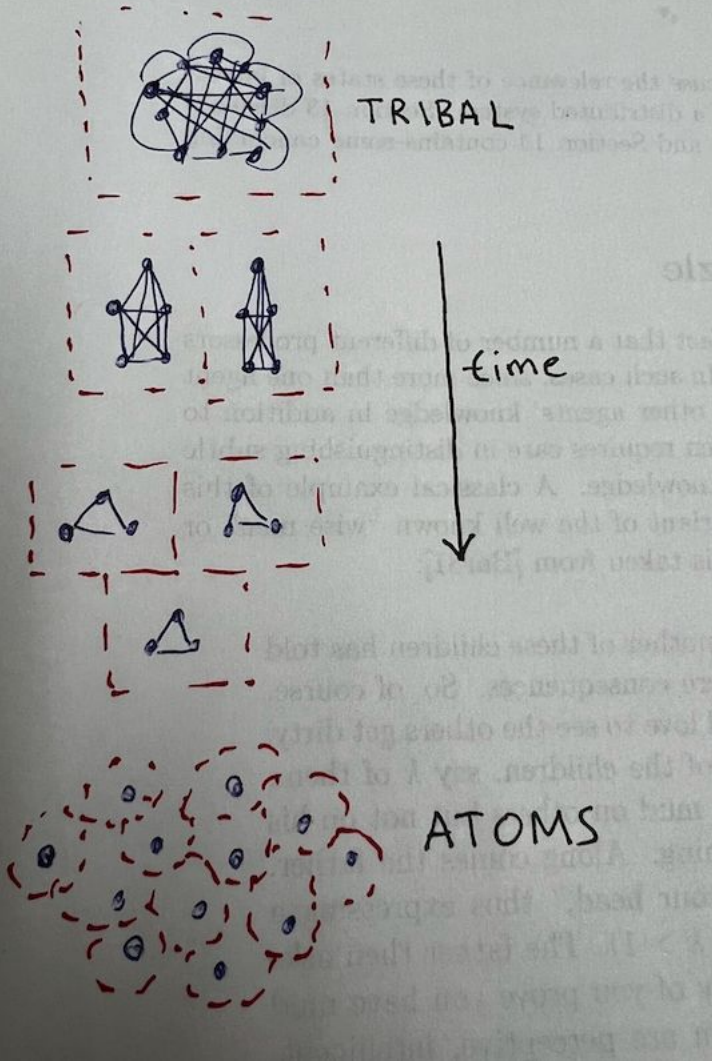
Gitcoin
leon@gitcoin.co

Glen Weyl

Microsoft, RadicalXChange
glen@radicalxchange.org

Context Collapse

- Used to have strong tribal bonds
- Communicate to invisible audiences today
- We have individual disclosure but lack collective disclosure



Designated Verifier Proofs

Instead of proving X ,

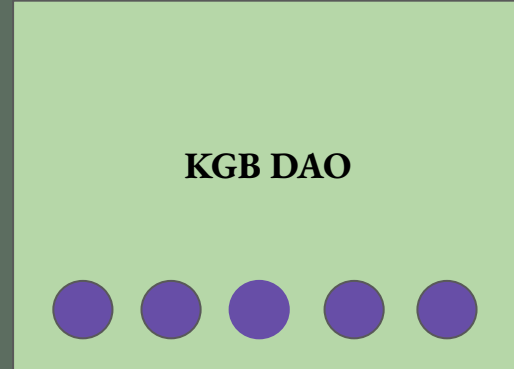
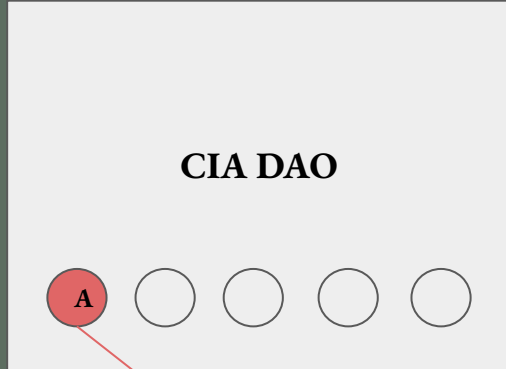
Alice will prove the statement "Either X is true or I am Bob."

Mitigate Probability Double Agents



Both groups want to prevent agents from spying on themselves.

Mitigate Probability Double Agents

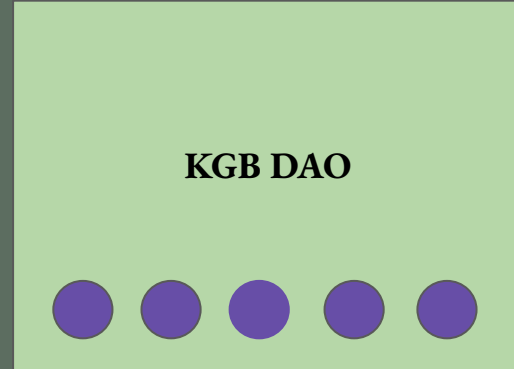


Agent A wants to turn on the CIA
& work for KGB, but the CIA
doesn't know this.

Mitigate Probability Double Agents



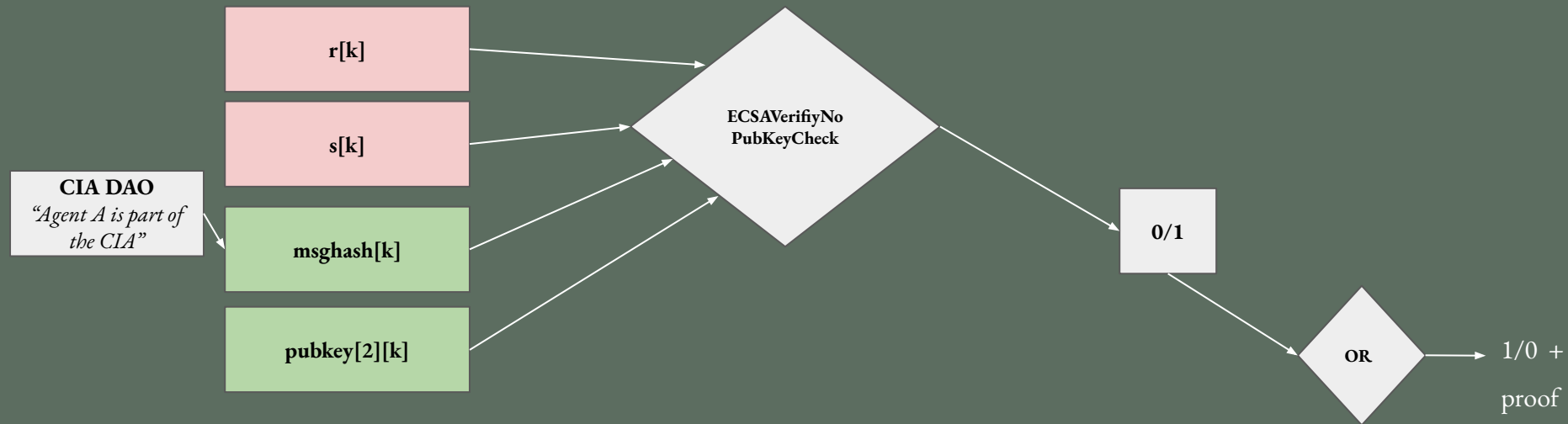
“Agent A is part of the CIA”



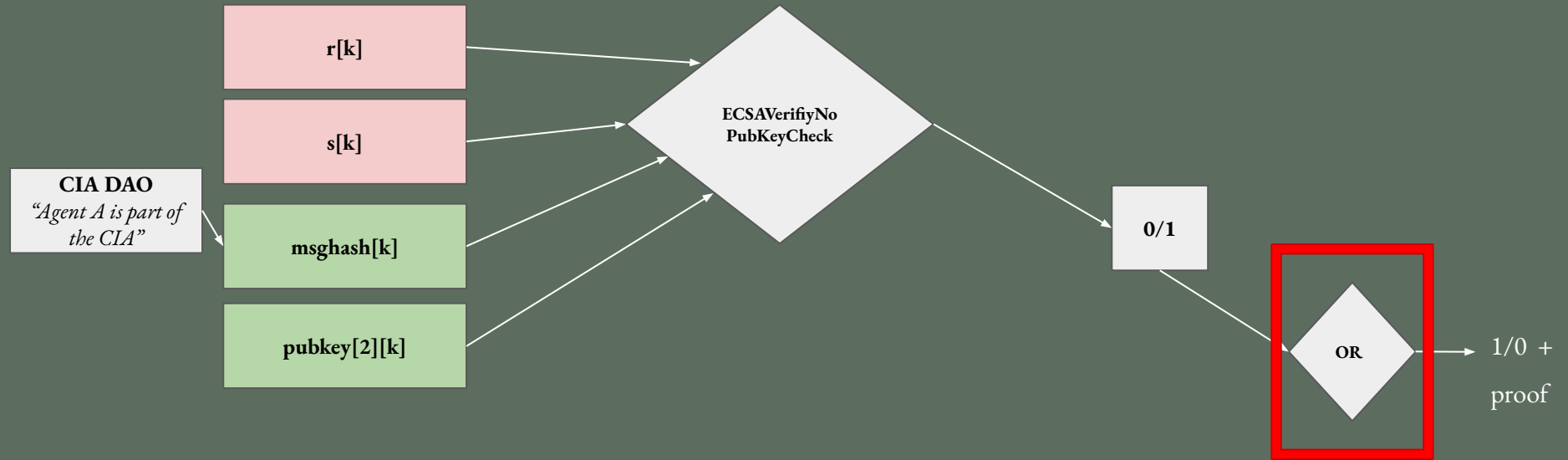
Does the KGB believe Agent A? How can we, the CIA,
mitigate the persuasiveness of this claim?

Designated Verifier Proof

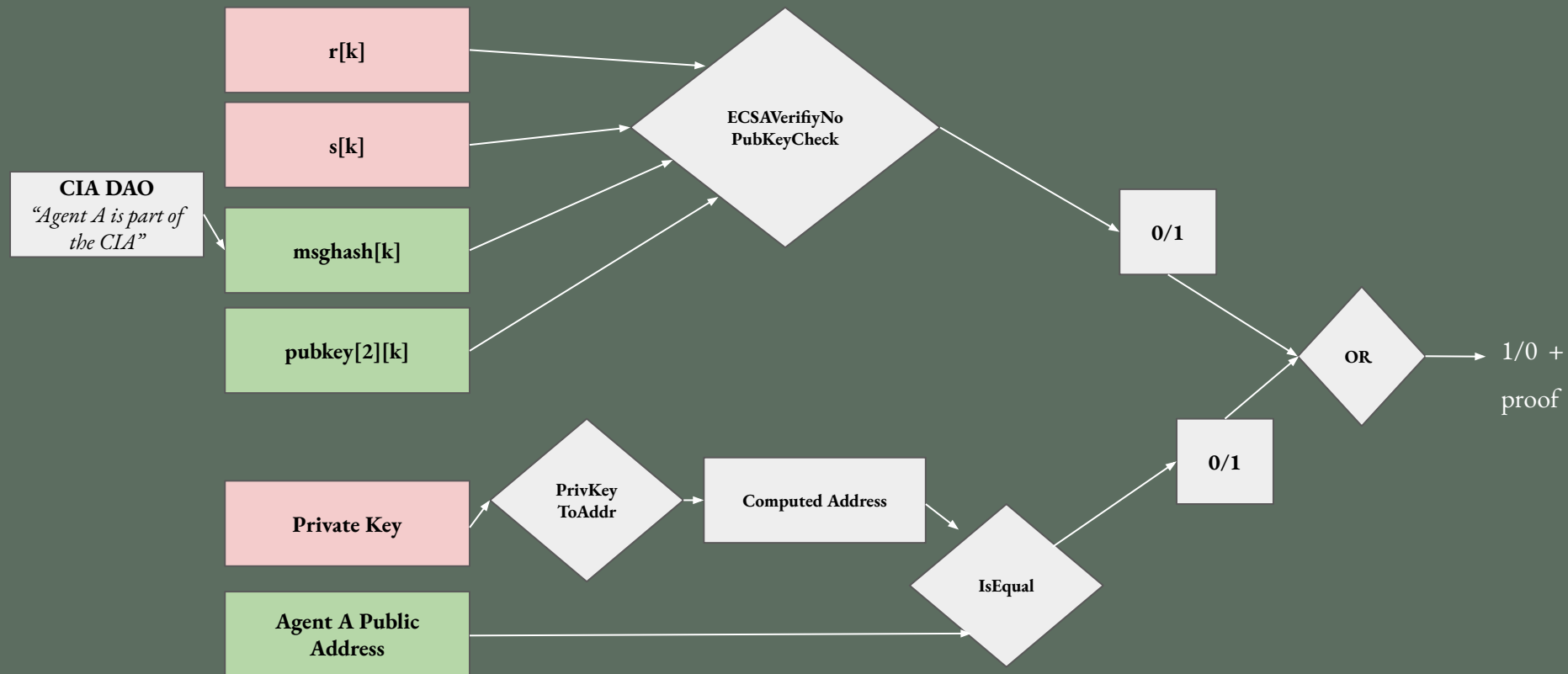
Designated Verifier Proof



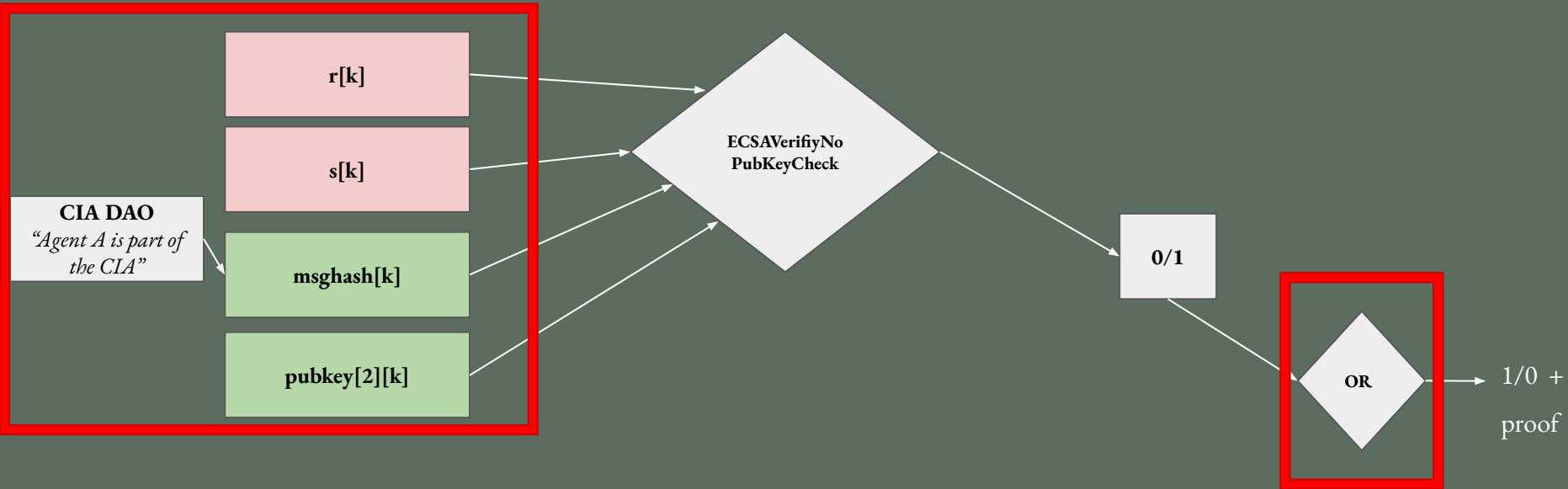
Designated Verifier Proof



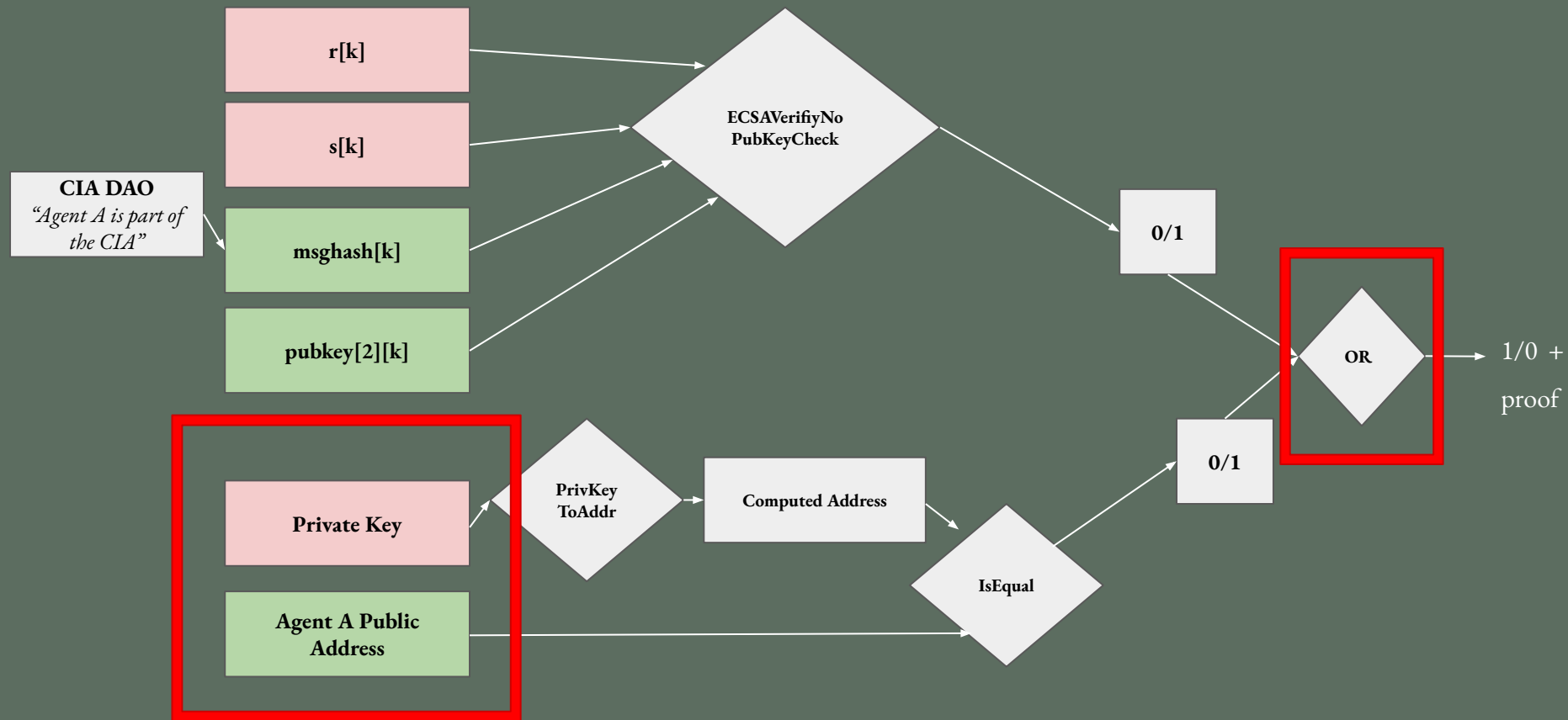
Designated Verifier Proof



Designated Verifier Proof



Designated Verifier Proof



You can't prevent someone from sharing information.

**However, you can prevent someone from making that
information be persuasive in its shared form!**

You can't prevent someone from sharing information.

However, you can prevent someone from making that information be persuasive in its shared form!

Collective Disclosure

DAO Intelligence

Timestep #1: DAO wants to share information with its DAO members.



Only DAO members and the DAO itself are persuaded by the DAO's claim about secret X. Any entity outside of the DAO is not persuaded.

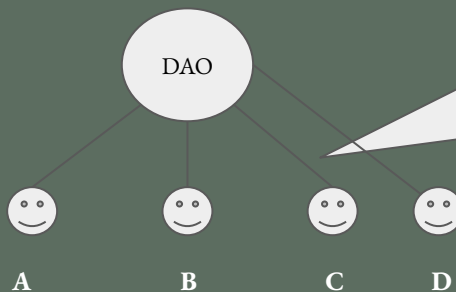
DAO Intelligence

Timestep #2: DAO wants to share information with another entity.

DAO Intelligence Proposal

Should entity D be aware of secret X?



If > threshold of members agree for this proposal to pass, proceed for the DAO to issue the DVP below.



DAO creates a DVP to each member's public address.

DVP for each member says "We have a secret X"

Open-Source Foundations


 README.md 


Designated Verifier Signatures

We have individual minimal disclosure. Designated Verifier Proofs (DVPs) enable collective minimal disclosure. In doing so, we can maintain the integrity of information within a set of selected agents. This repository is designed to enable people to build DVPs into their social applications and can be done both on and off-chain. It is designed to be compatible for EVM based applications.

[Publish your first package](#)

Contributors 2

 **enricobottazzi** Enrico Bottazzi

 **shreyjain13** Shrey Jain



The State Today

- We lack systems to attain common-p belief
- We lack systems to provide context
- We need boundaries

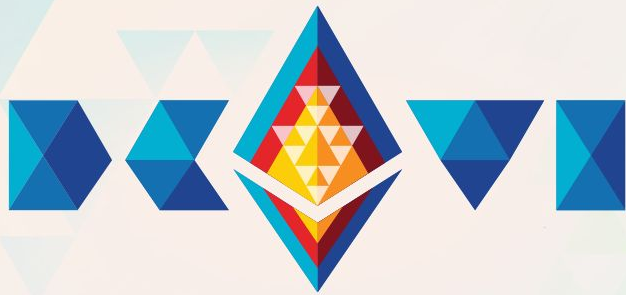


What we can build?

- DVP protocol for DAO intelligence
- Commitment schemes
- Tools for anonymous reporting
- Collective action protocols for social movements



Let's interweave cryptographic
primitives with cultural
communities!



Thank you!

Shrey Jain

Web3 Researcher, Microsoft

shreyjaineth@gmail.com



@shreyjaineth