Proof of Novelty

A distributed consensus mechanism for securing content novelty

Daniel Severo

Independent Scientist

Virtual Design Challenge
The University of British Columbia
Vancouver - December 2019

Table of Contents

Target audience: undergraduate students in STEM with a basic knowledge of Blockchain technology.

Table of Contents

Motivation

Motivational question

Somebody sends you a video, how do you know it is *trustworthy*?

Motivation

Motivational question

Somebody sends you a video, how do you know it is *trustworthy*?

- Existing content can be manipulated for ill-usage.

Figure: Obama speech out of context.

Table of Contents

Trustworthiness

What does it mean to trust content?

Trustworthiness

What does it mean to trust content? Usually, we want *novelty* and *authenticity*.

Trustworthiness

What does it mean to trust content? Usually, we want *novelty* and *authenticity*.

Authenticity

Trustworthiness

What does it mean to trust content? Usually, we want *novelty* and *authenticity*.

Authenticity

- Content is authentic when its origin is indisputable.

Trustworthiness

What does it mean to trust content? Usually, we want *novelty* and *authenticity*.

Authenticity

- Content is authentic when its origin is indisputable.
- Can be reasonably solved with Digital Signatures.

Trustworthiness

What does it mean to trust content? Usually, we want *novelty* and *authenticity*.

Authenticity

- Content is authentic when its origin is indisputable.
- Can be reasonably solved with Digital Signatures.
- Easy to check, since verifying signatures is fast.

Trustworthiness

What does it mean to trust content? Usually, we want *novelty* and *authenticity*.

Authenticity

- Content is authentic when its origin is indisputable.
- Can be reasonably solved with Digital Signatures.
- Easy to check, since verifying signatures is fast.

Novelty

Trustworthiness

What does it mean to trust content? Usually, we want *novelty* and *authenticity*.

Authenticity

- Content is authentic when its origin is indisputable.
- Can be reasonably solved with Digital Signatures.
- Easy to check, since verifying signatures is fast.

Novelty

- Subjective in nature, depends on the context.

Trustworthiness

What does it mean to trust content? Usually, we want *novelty* and *authenticity*.

Authenticity

- Content is authentic when its origin is indisputable.
- Can be reasonably solved with Digital Signatures.
- Easy to check, since verifying signatures is fast.

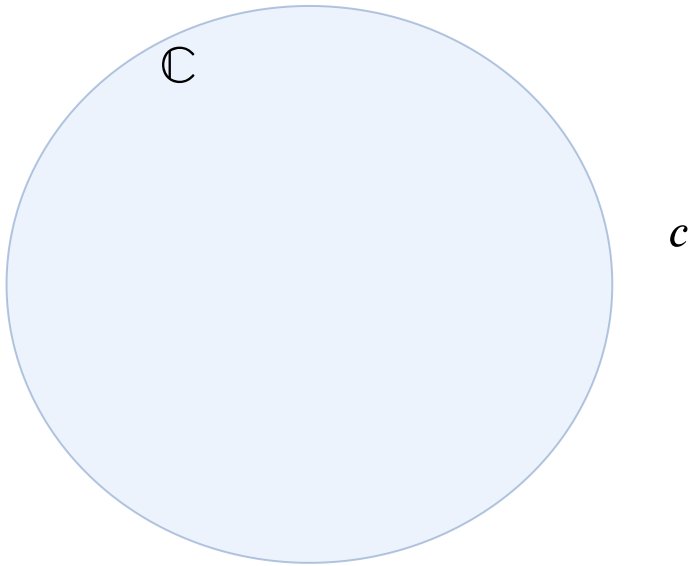
Novelty

- Subjective in nature, depends on the context.
- Hard to check, requires comparing against archives.

Table of Contents

Proof of Novelty

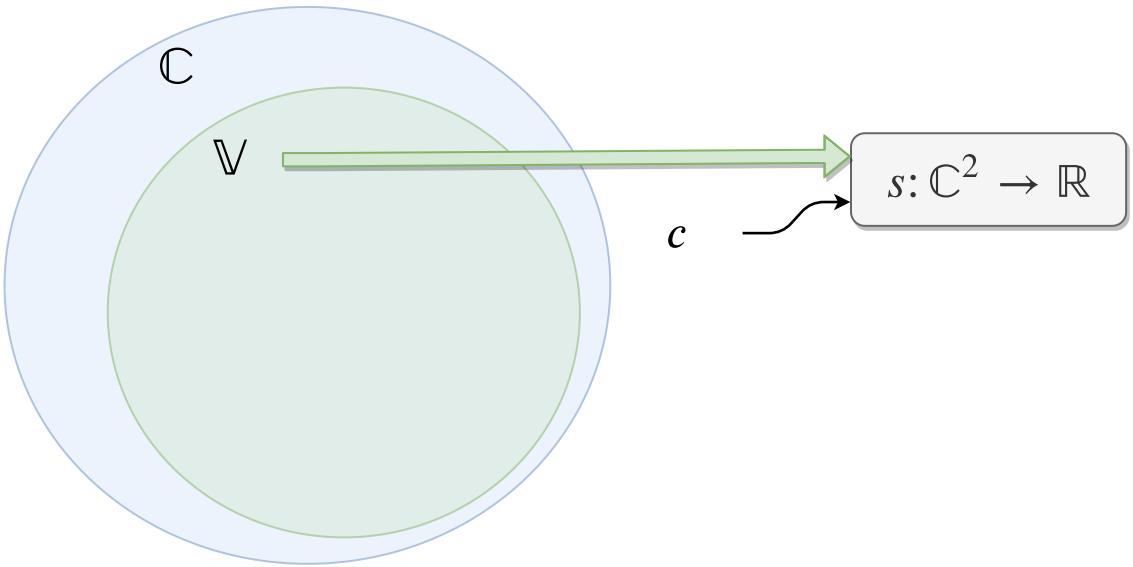
1. The owner of content c wishes to prove to us it is trustworthy.
2. A collection of similar content $\mathbb{C}$ exists and is secured on a blockchain with content-addressable hashes.



Proof of Novelty

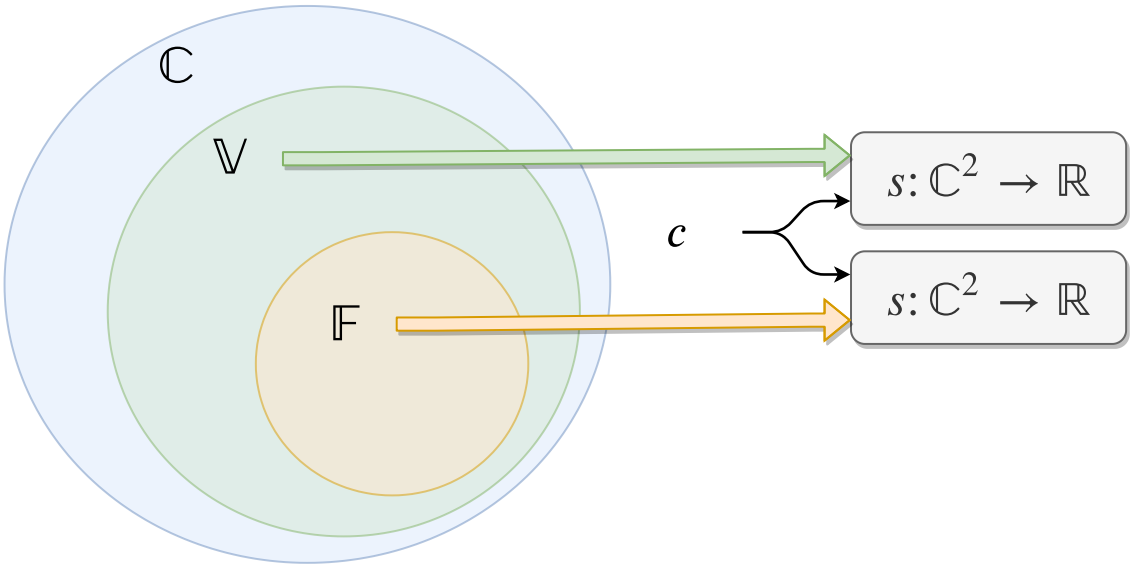
3 The owner makes a transaction on the blockchain and receives a random subset of content-hashes $\mathbb{V} \subseteq \mathbb{C}$.

4 The owner calculates the similarity of c with the elements of $\mathbb{V}$, using a predefined similarity measure.



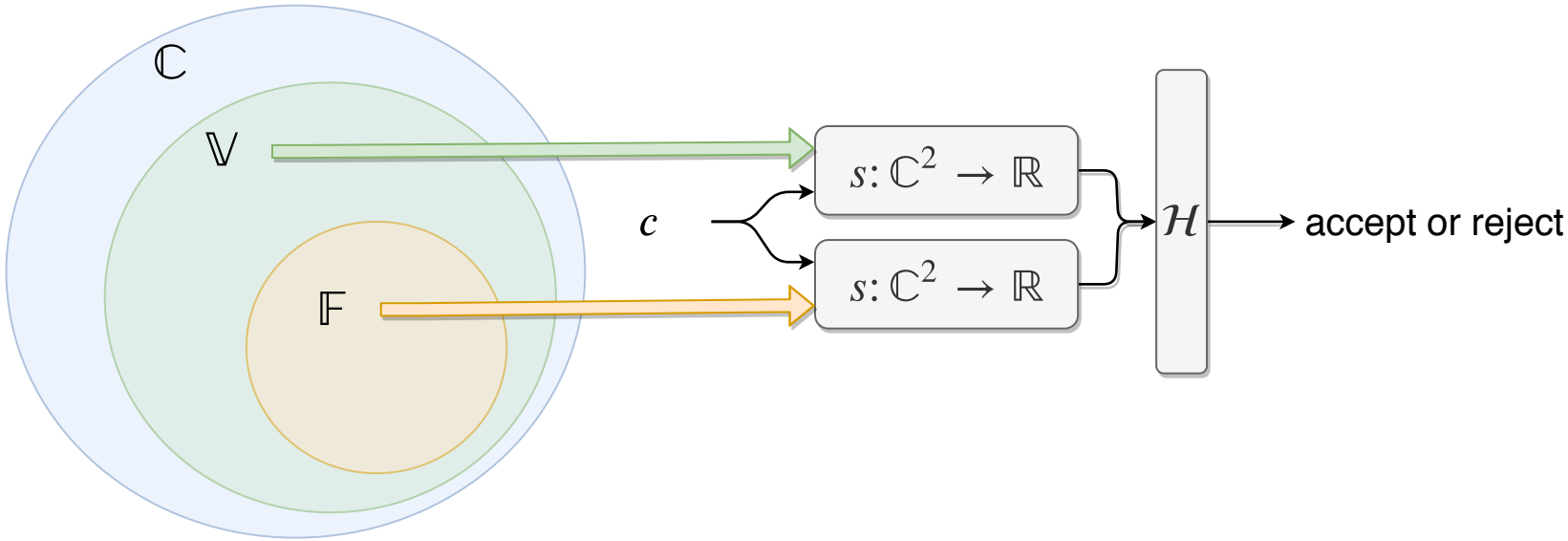
Proof of Novelty

5 The blockchain chooses a random committee of peers that verify a subset of the results, $\mathbb{F} \subseteq \mathbb{V}$.



Proof of Novelty

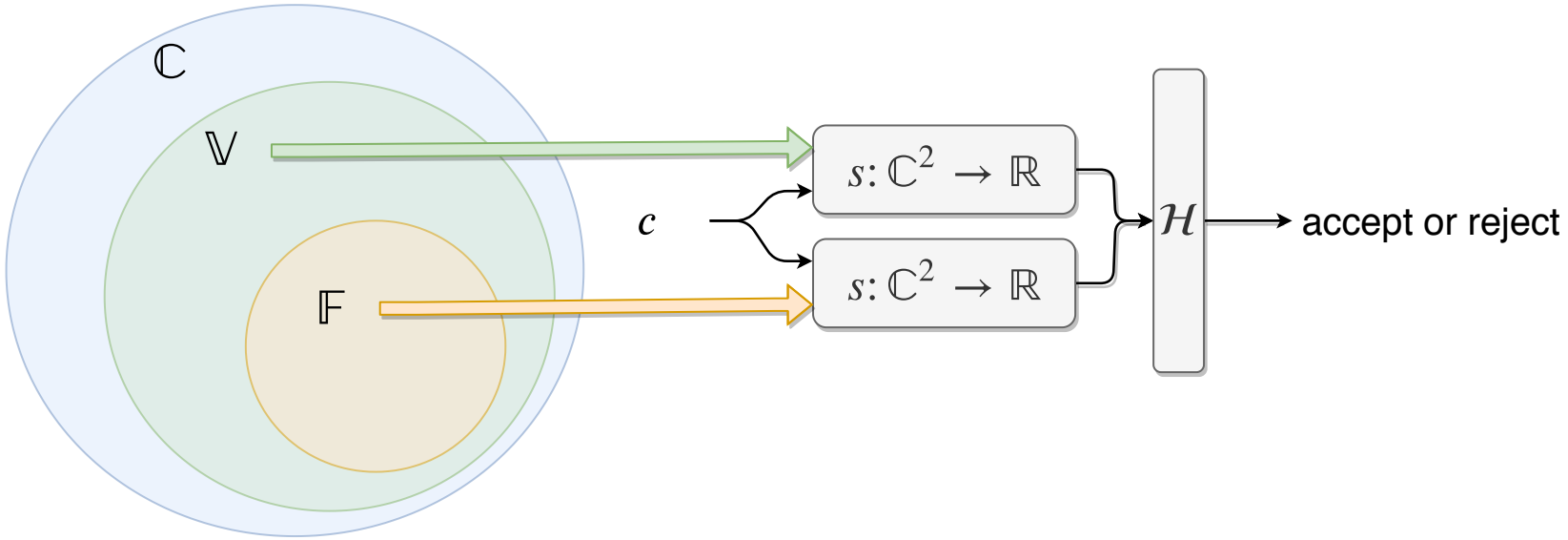
6 Consensus is reached by the committee regarding the legitimacy of the owner's calculations, and c is accepted or rejected into $\mathbb{C}$.



System details

Creating $\mathbb{F}$ through sortition

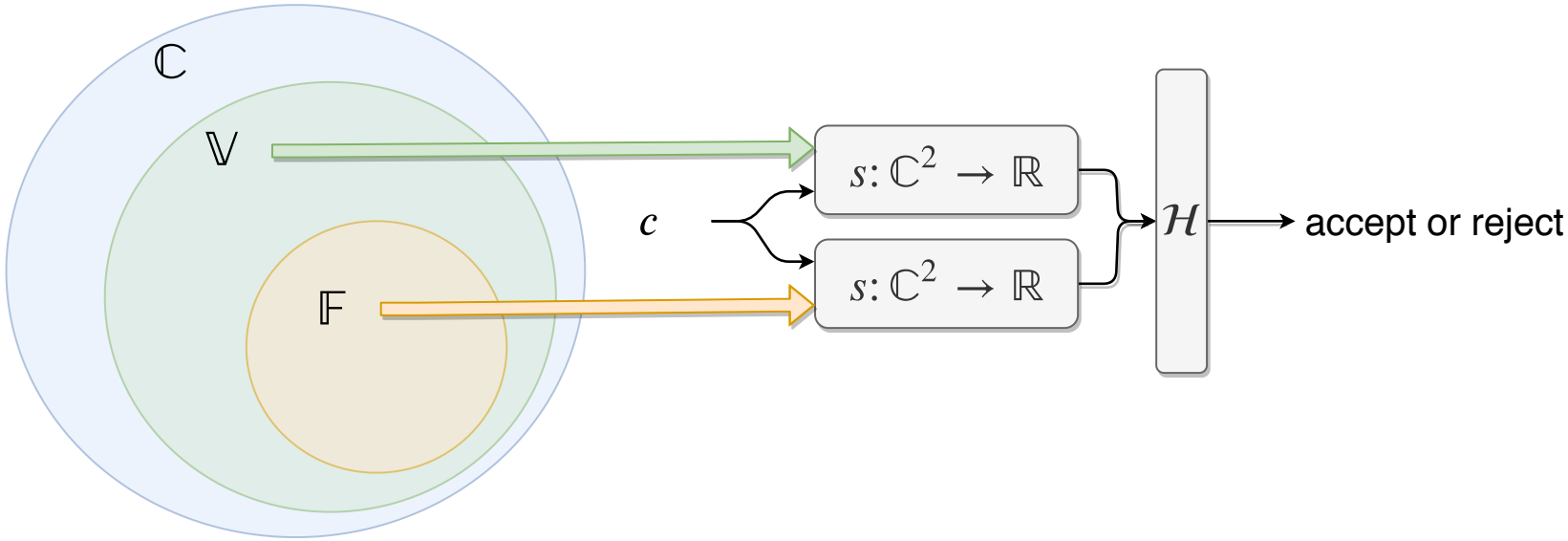
Cryptographic Sortition can form committees without the need of interactions or exposure. Any peer holding a private key can verify and prove self-membership in the committee using a *Verifiable Random Function*.



System details

Similarity measure $s\colon \mathbb{C}^2 \to \mathbb{R}$

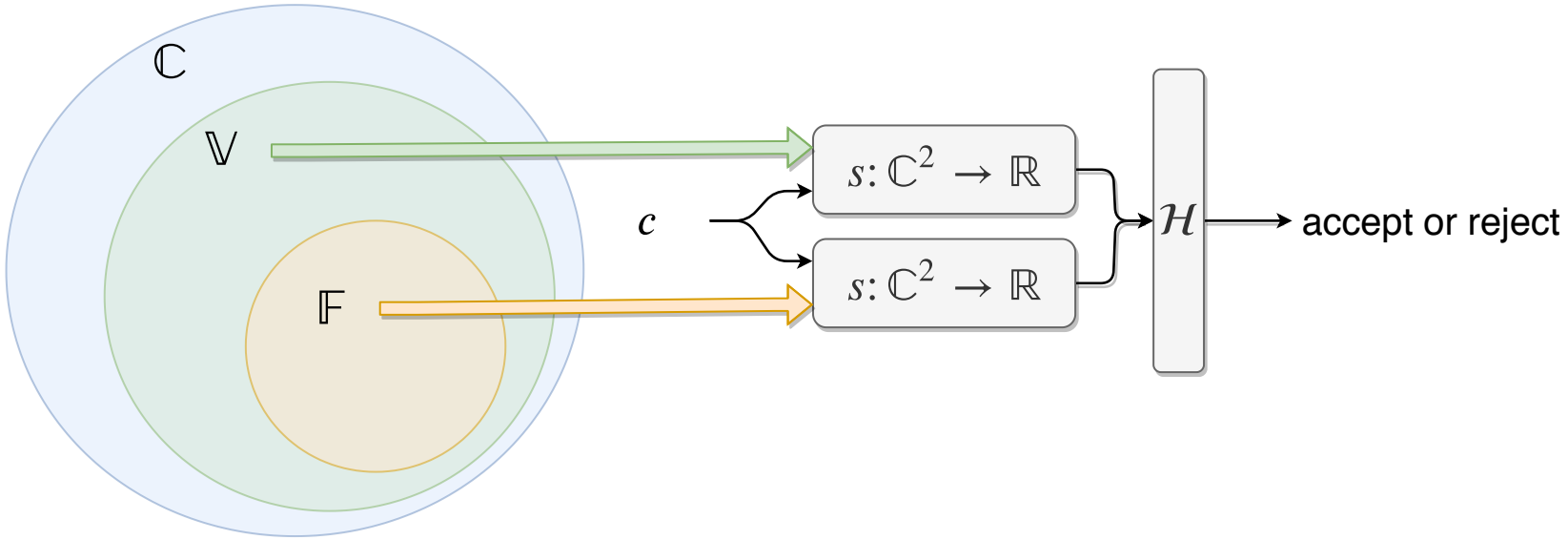
A similarity measure is any function that quantifies the degree of similarity between objects, such as a *Neural Network*.



System details

Evaluating the owner's submitted results

The committee must estimate if the similarity calculations between c and elements of $\mathbb{V}$ are legitimate, by observing only $\mathbb{F}$.



Probabilistic Guarantee of Novelty

If the owner's content is accepted, it provides a *probabilistic guarantee* that their content is novel.

Table of Contents

Take-away points

Proof of Novelty ...

- is a certificate issued by a decentralized and trustless system;

Take-away points

Proof of Novelty ...

- is a certificate issued by a decentralized and trustless system;
- provides probabilistic guarantees of content novelty;

Take-away points

Proof of Novelty ...

- is a certificate issued by a decentralized and trustless system;
- provides probabilistic guarantees of content novelty;
- can scale by using cryptographic sortition;

Take-away points

Proof of Novelty ...

- is a certificate issued by a decentralized and trustless system;
- provides probabilistic guarantees of content novelty;
- can scale by using cryptographic sortition;
- defines similarity through similarity measures;

Take-away points

Proof of Novelty ...

- is a certificate issued by a decentralized and trustless system;
- provides probabilistic guarantees of content novelty;
- can scale by using cryptographic sortition;
- defines similarity through similarity measures;
- can be extended to any content type by switching the similarity measure.

Table of Contents

Open Questions and Future Work

- Implementing and running experiments on Smart Contract blockchains such as Ethereum;

Open Questions and Future Work

- Implementing and running experiments on Smart Contract blockchains such as Ethereum;
- Applying decentralized and collaborative machine learning to progressively update a similarity function;

Open Questions and Future Work

- Implementing and running experiments on Smart Contract blockchains such as Ethereum;
- Applying decentralized and collaborative machine learning to progressively update a similarity function;
- Investigating statistical hypothesis tests and guarantees for different content and similarity functions;

Open Questions and Future Work

- Implementing and running experiments on Smart Contract blockchains such as Ethereum;
- Applying decentralized and collaborative machine learning to progressively update a similarity function;
- Investigating statistical hypothesis tests and guarantees for different content and similarity functions;
- Properly choosing $\mathbb{V}$ and $\mathbb{F}$ to optimize statistical and computational performance.

Thank you!

- _dsevero
- dsevero
- → dsevero.com

For references, see the original paper at github.com/dsevero/Proof-of-Novelty