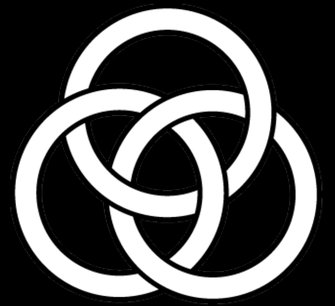
Deterministic Hashed Data Elision

Problem Statement & Areas of Work



Shannon Appelcline, Tech Writer at Blockchain Commons

Data is

The Problem

- Poor Data Control
- Poor Data Privacy
- No Human Rights

Challenge #1

Disclosure

Data Says More than It Needs To

Challenge #2

Correlation

Discrete Data Can Be Aggregated

Challenge #3

Secondary Use

Data Is Used for Something Other than Intended

These Challenges Are Cumulative

More Data Disclosed ➡

More Data Correlated ➡

More Secondary Use ➡

More Problems! ☣

The Data Problem is

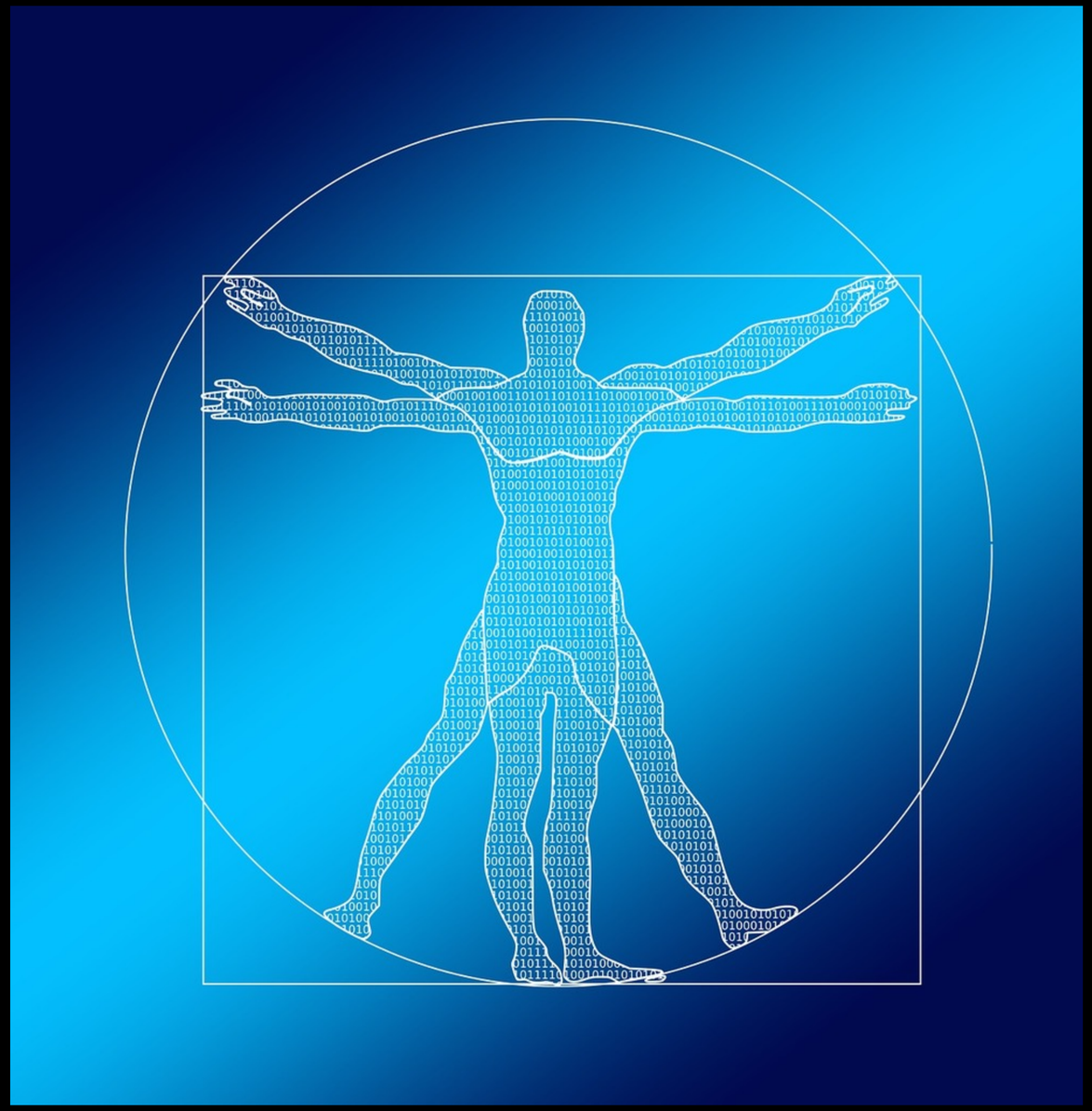
Growing Larger

- More Data is Being Collected
- More Data is Online
- More Data is Sensitive

Digital Identity

Makes Data Problems Bigger Still

- Decentralized Identifiers (DIDs)
- Mobile Driver Licenses (MDLs)
- EU’s eIDAS
- Forums, Utilities, Banks, Social Media, Online Shopping, Airlines, Newspapers … it’s all Identity!
    - I have 410 accounts!
      (that I remember)



Data
Is Everywhere

- Credentials
- Financial Industry
- Health Care
- Supply Chain
- Software Releases

We Need to Get in Front of The Problem

IETF Has Solutions

RFC 6973: Privacy Considerations for Internet Protocols
RFC 8280: Research into Human Rights Protocol Considerations

July 2013

Abstract

This document offers guidance for developing privacy considerations for inclusion in protocol specifications. It aims to make designers, implementers, and users of Internet protocols aware of privacy-related design choices. It suggests that whether any individual RFC warrants a specific privacy considerations section will depend on the document's content.

RFC 6973

Privacy Considerations for Internet Protocols

October 2017

Abstract

This document aims to propose guidelines for human rights considerations, similar to the work done on the guidelines for privacy considerations (RFC 6973). The other parts of this document explain the background of the guidelines and how they were developed.

This document is the first milestone in a longer-term research effort. It has been reviewed by the Human Rights Protocol Considerations (HRPC) Research Group and also by individuals from outside the research group.

RFC 8280

Research into Human Rights Protocol Considerations

RFCs 6973 & 8280

Aren’t Securing Data

- They’re Somewhat Dated
- They’re Not Concrete
- They’re Not Required
- They’re Not Used

RFC 6973

Privacy Recommendations

- Anonymity (§6.1.1)
- Pseudonymity (§6.1.2)
- Data Minimization (§6.1)

Anonymity / Pseudonymity

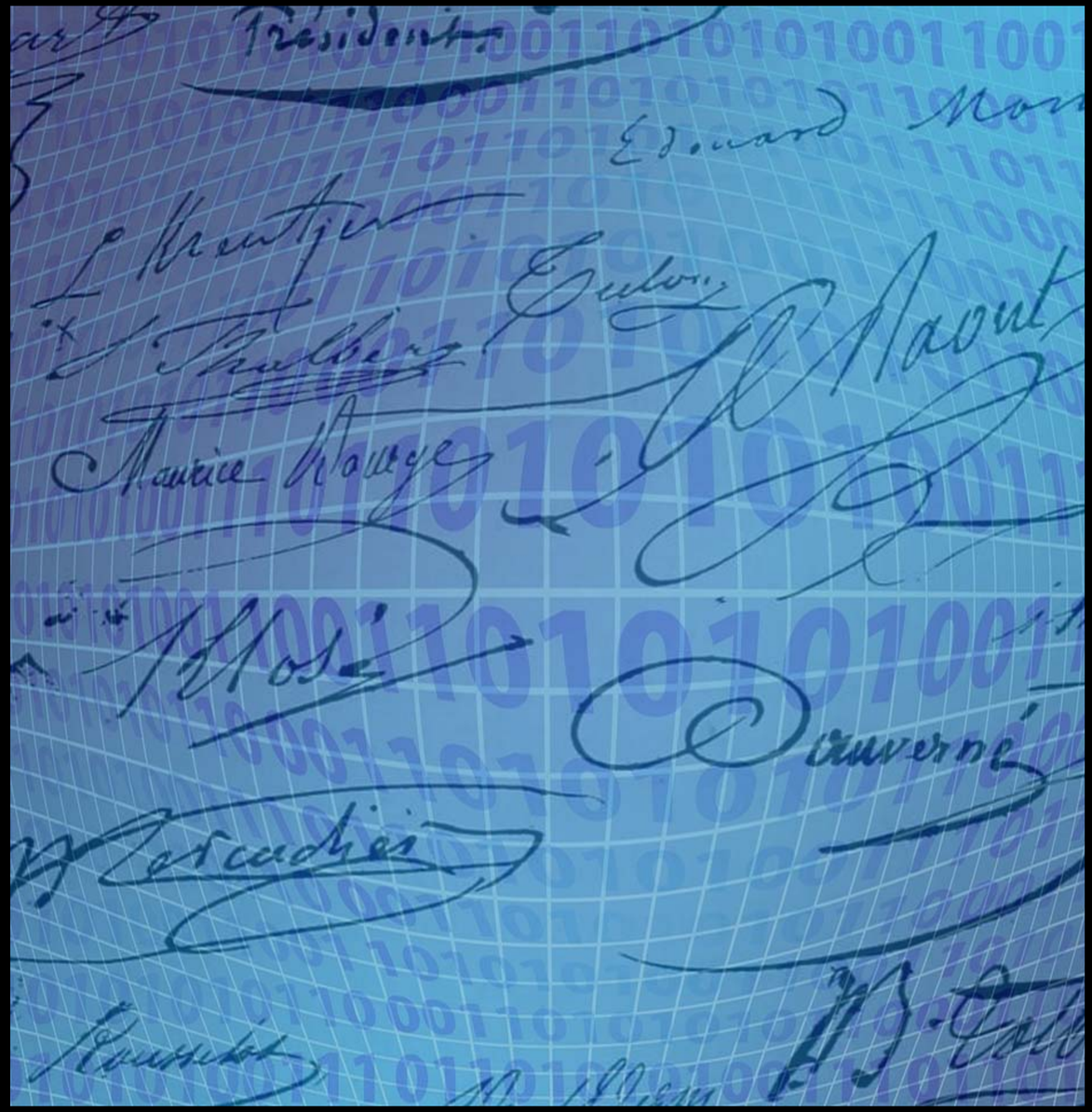
Privacy Problems

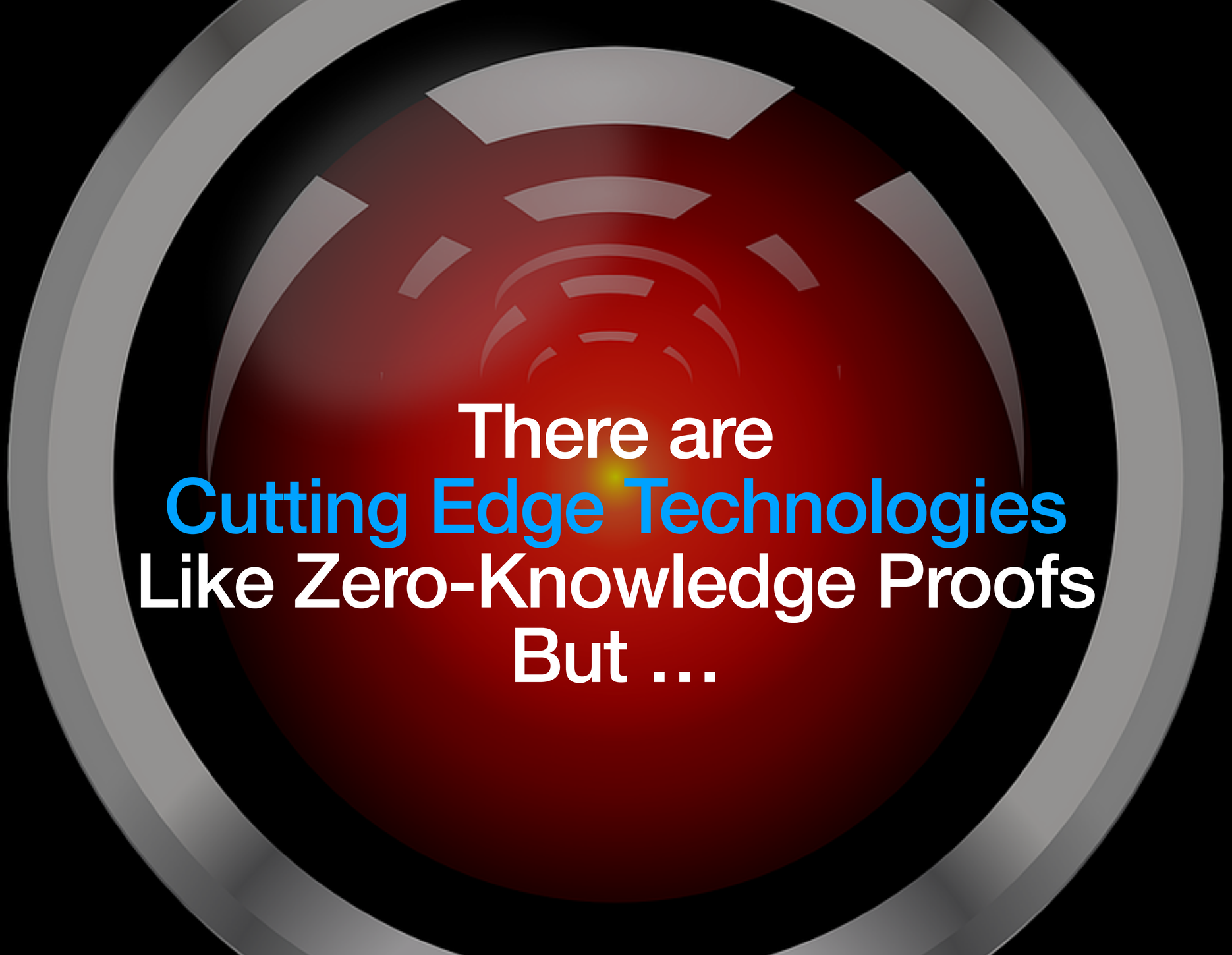
- They’re Insufficient
- Can Still Have Too Much Disclosure
- Can Still Have Correlation
- Can Still Have Secondary Use

Data Minimization

Human Rights Problems

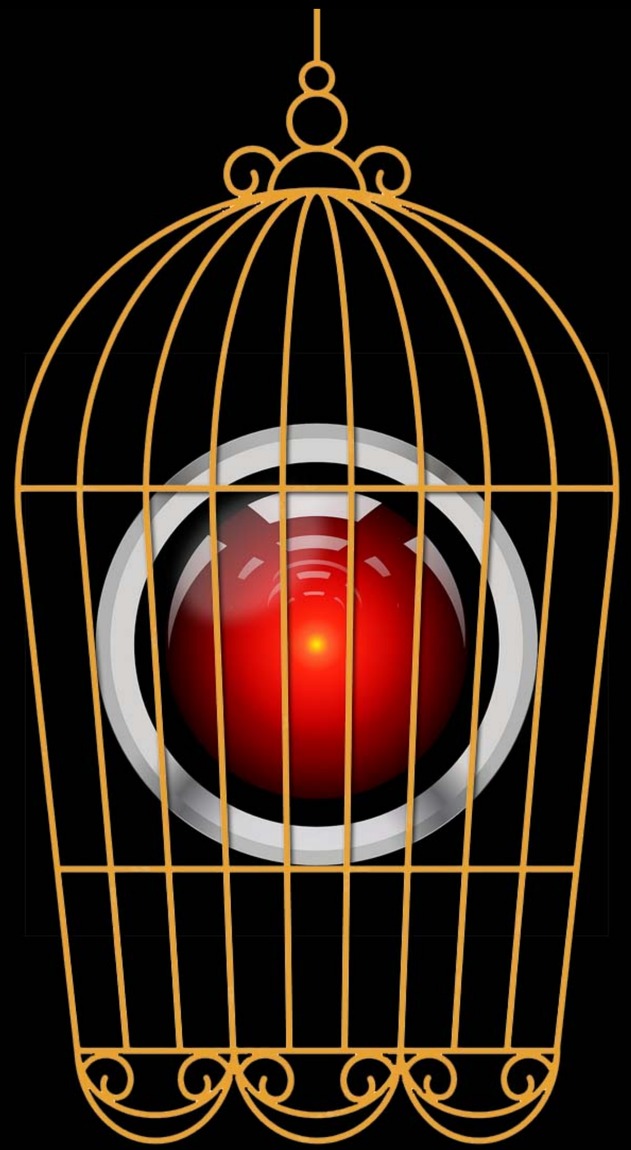
- Classic Data Minimization Violates Human Rights
- No Authenticity
    - *RFC 8280 §6.2.17*
- No Integrity
    - *RFC 8280 §6.2.16*
- No Decentralization
    - *RFC 8280 §6.2.13*




There are
Cutting Edge Technologies
Like Zero-Knowledge Proofs
But …

We Need Privacy Tech That Is

- Simple
- Well Understood
- In Production
- But More Advanced than 2013



We Need a Middle Ground

Deterministic Hashed Data Elision

Is that Middle Ground

Deterministic

Data is always organized the same.

Hashed

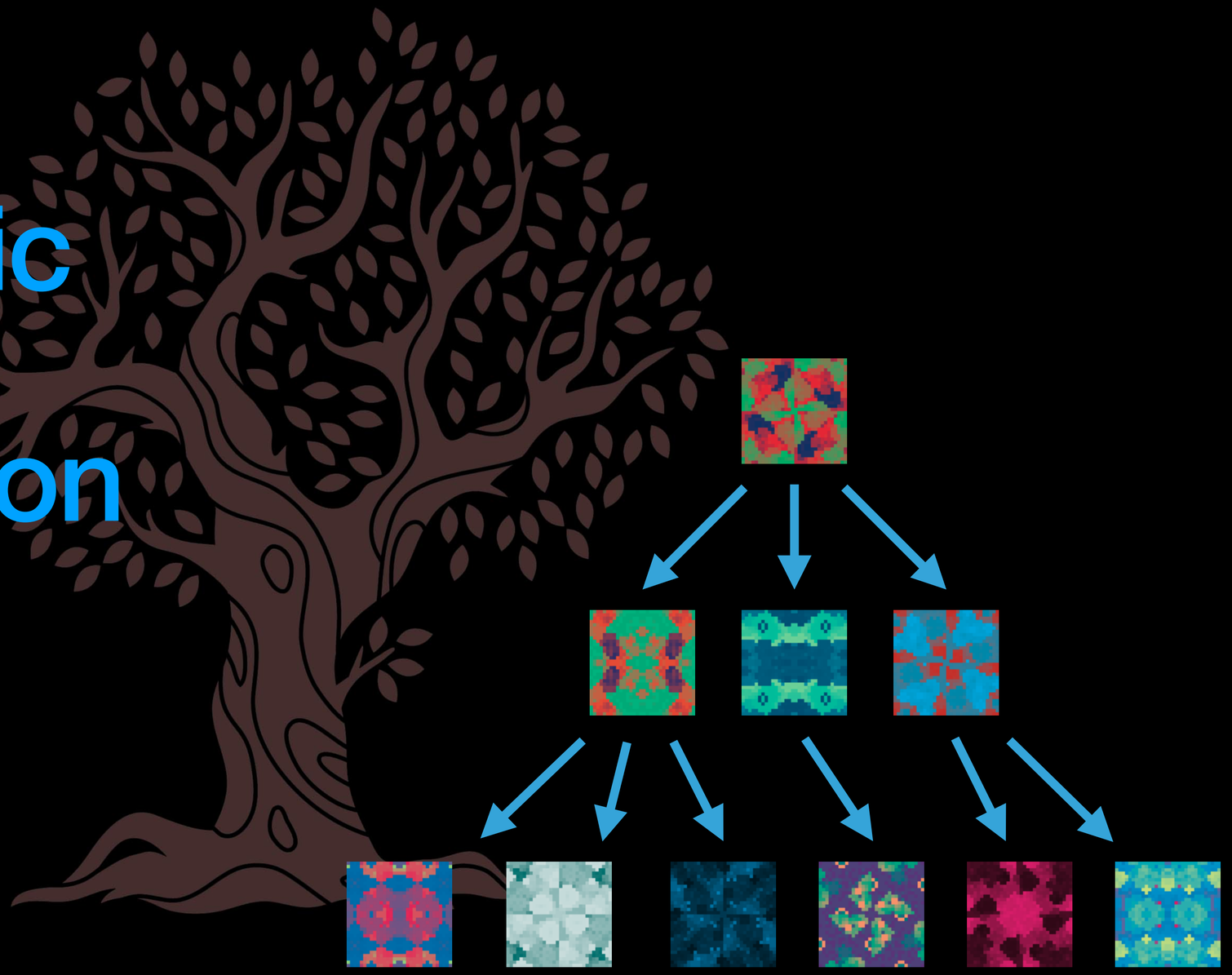
A hash is stored for each data leaf.

Data Elision

Data can be removed by any holder.

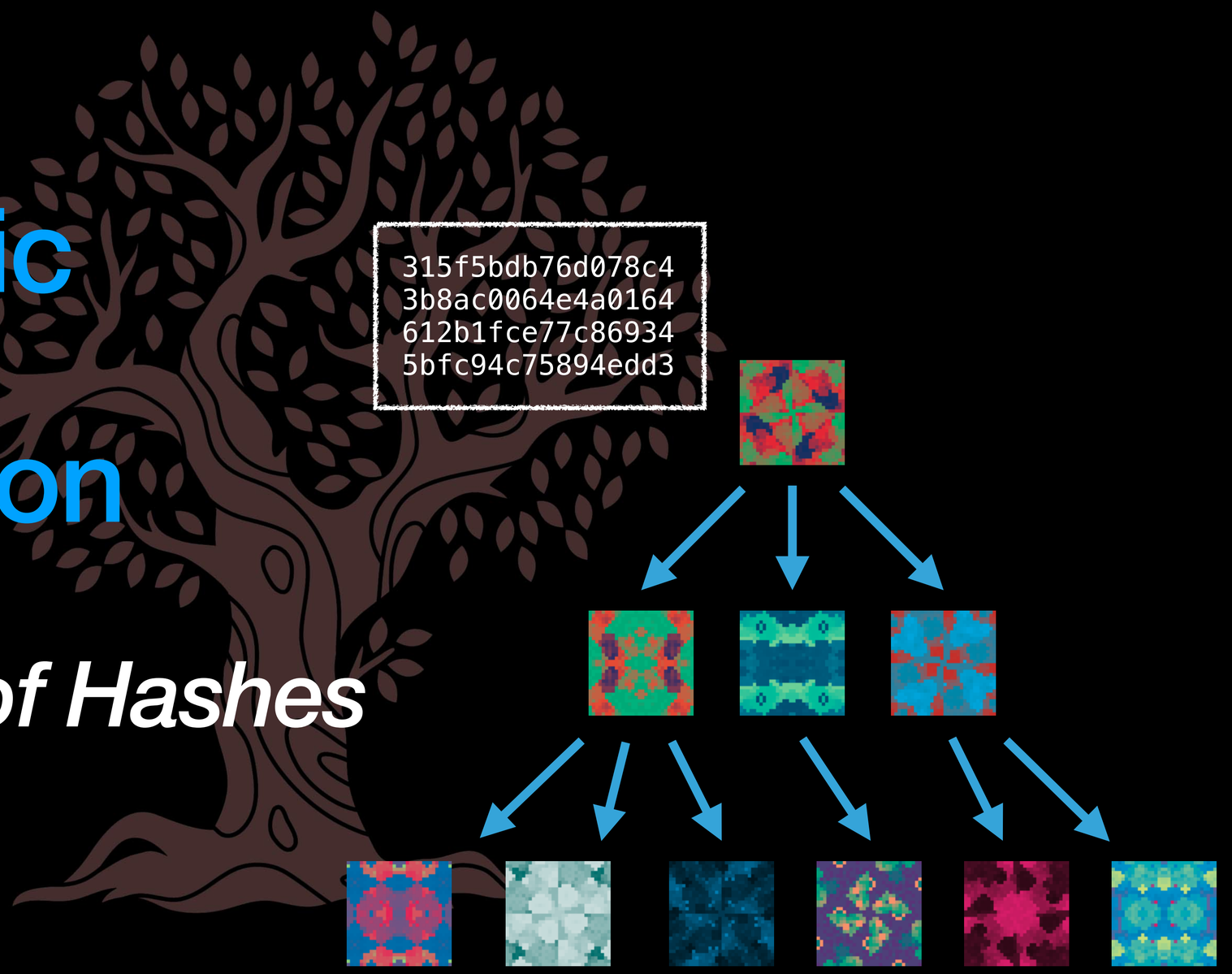
Deterministic Hashed Data Elision

A Merkel Tree



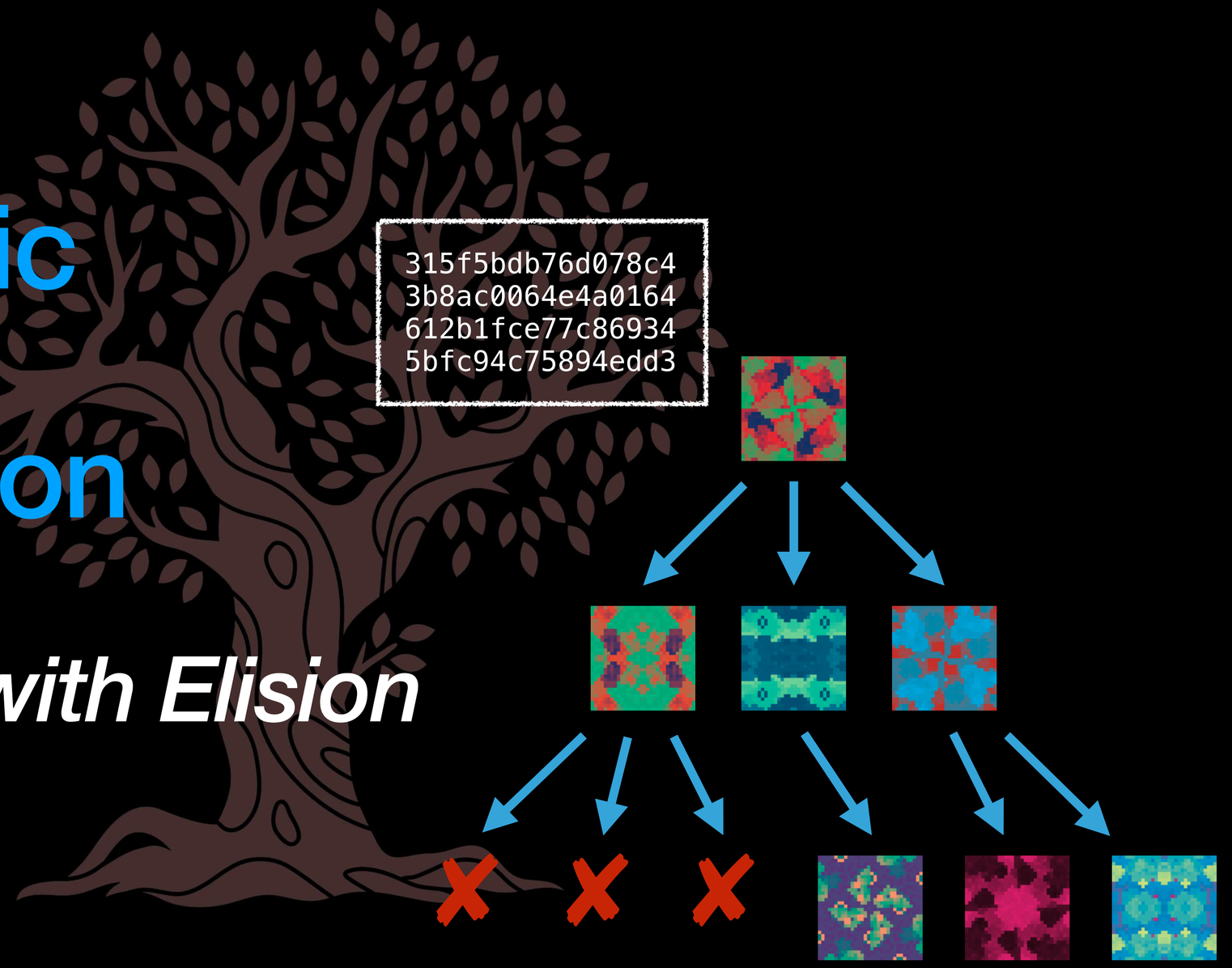
Deterministic Hashed Data Elision

A Merkel Tree of Hashes



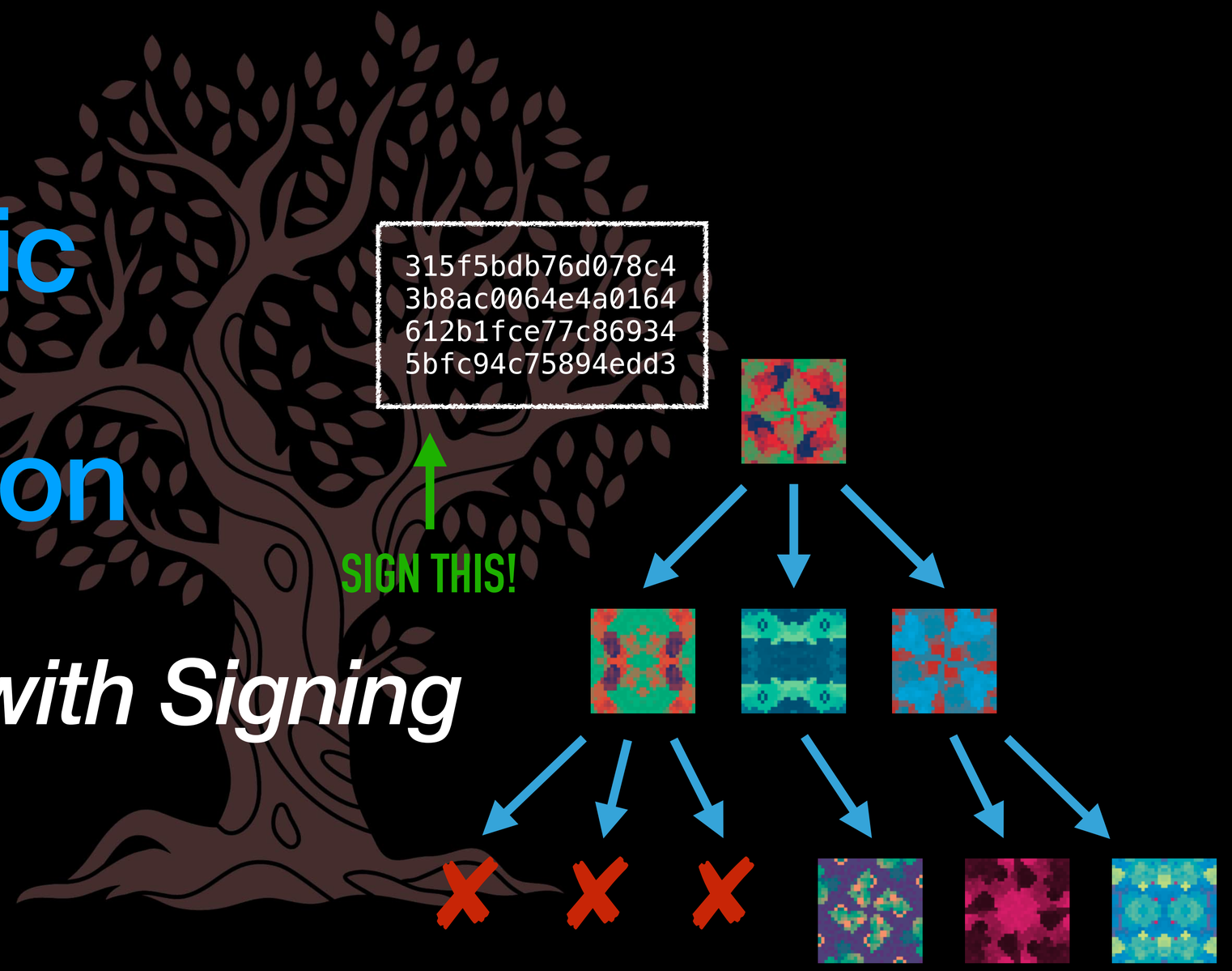
Deterministic Hashed Data Elision

A Merkel Tree with Elision



Deterministic Hashed Data Elision

A Merkel Tree with Signing



Advantages of Deterministic Hashed Data Elision

- Holder Agency
- Minimized Data
- Validated Signatures

Advantages of Deterministic Hashed Data Elision

- Holder Agency
- Minimized Data
- Validated Signatures
- Inclusion Proofs
- Herd Privacy

Advantages of Deterministic Hashed Data Elision for Correlation

To Correlate or Not to Correlate?

- Use the Best Hash for Your Needs!
- Traditional Hashes
  - SHA-256
- Salted Hashes
- Advanced Hashes
  - HMAC
  - Oblivious PRF

Advantages of Deterministic Hashed Data Elision

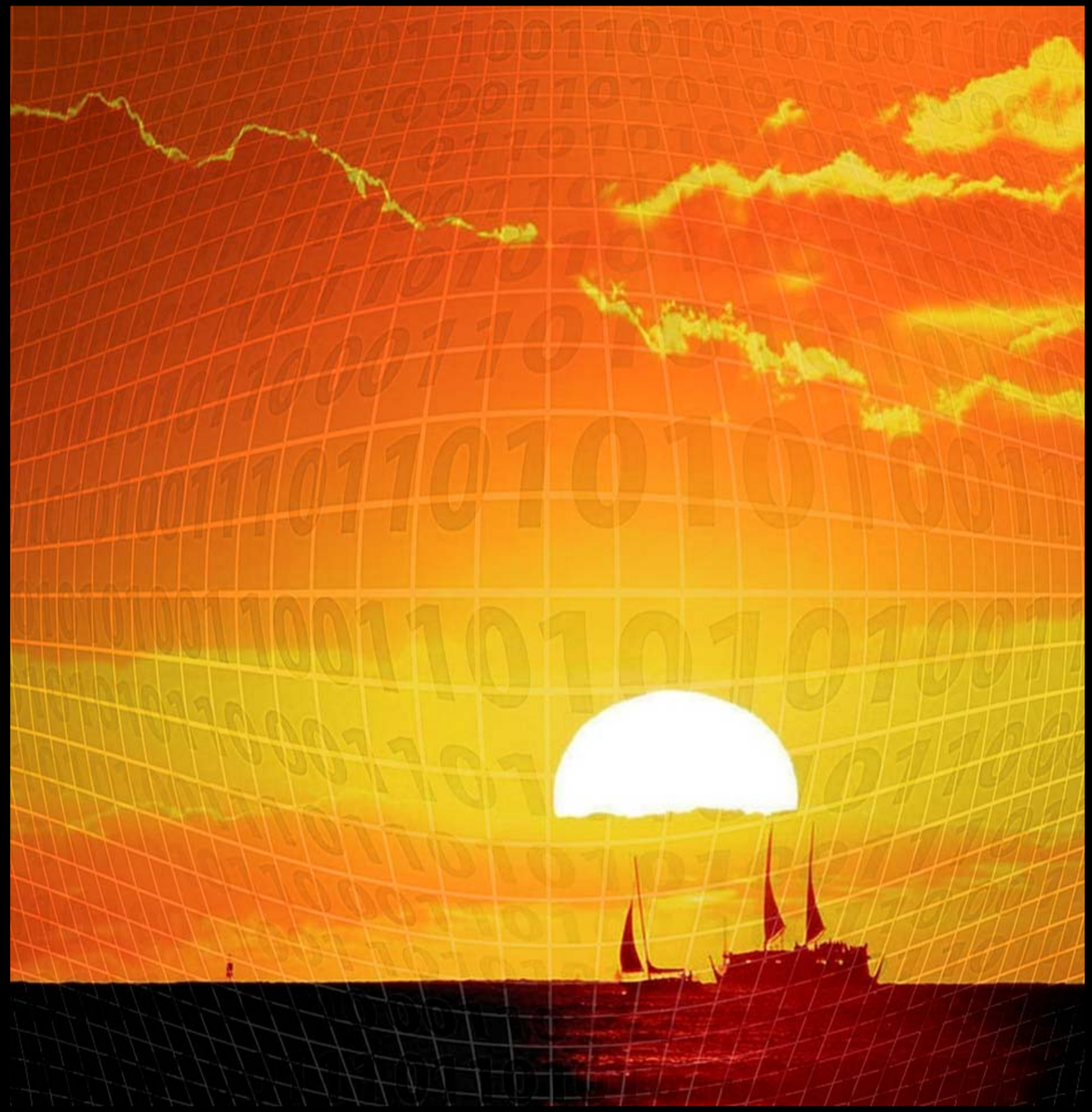
- Fulfills RFC 6973
- Fulfills RFC 8280
- Supports Authenticity
- Supports Decentralization
- Supports Integrity

Deterministic Hashed Data Elision

is Important!

We’d love to see it incorporated into IETF protocols in whatever form is desired.

- Credentials
- Data Provenance
- Digital Assets
- Healthcare
- Software Signing
- More



Gordian Envelope

is Our Own Implementation

Additionally Supports:

- *Many forms of Structured Data including multiple kinds of graphs*
- *Optionally salted hashes*
- *Encryption*
- *Expressions (Functions)*
- *Other cryptographic data*

Our Questions for Dispatch

Where can we advance issues of these sorts?

- There’s not currently a good venue!

How can we work on data privacy & human rights in a practical way?

- RFCs 6973 & 8280 are largely ignored.
- How can the IETF do better?

- The need for deterministic hashed data elision is ubiquitous!
- Everyone should be a customer!

Should we create a group to focus on data minimization of all sorts for data at rest?

- Deterministic hashed data elision could be one of many solutions.
- We'd like to see them get more attention.

- Should This Be CFRG?
- Do we run a BoF toward a new Working Group?
- Do we join another group?

How do we bring attention to our own work specifically on Gordian Envelope?

- We'd done great work with the CBOR group revising it.
  - But they believe they're not ultimately the right venue.

- Some say we should try COSE
  - They have legacy constraints. Elision in SD-CWT is useful, but limited.

- Do we try to form a working group specific for Gordian Envelope?
- Or do we try advance the Envelope I-D as an an informational RFC with support from an Area Director?

For More Info

- draft-appelcline-hashed-elision
- draft-mcnally-envelope

Thank You!

SHANON APPELCLINE
shannon.appelcline@gmail.com

CHRISTOPHER ALLEN
christophera@blockchaincommons.com

@BlockchainComns

List of Envelope resource links:

https://www.blockchaincommons.com/introduction/Envelope-Intro/#envelope-links