



AUTHENTICITY-BY-DESIGN
FALL SEMINAR SERIES

Oct 31 **CAPTURE - New Tools to Establish Trust**
Tue 12pm to 1pm | Green Library | Hohbach Hall 122

Nov 7 **STORE - Authenticated Databases**
Tue 12pm to 1pm | Paul G. Allen Center 101X

Nov 30 **VERIFY - Applying Authenticity**
Tue 12pm to 1pm | Packard 204



Join in person at Stanford University -OR- remote on Zoom

AUTHENTICATED ATTRIBUTES

Kate Sills for Starling Lab
katelynsills.com
11-07-2023



TIME

How to Spot an AI-Generated Image Like the 'Balenciaga Pope'

A closer look at the Balenciaga Pope image

His **eyelid** appears to merge into his glasses then flow into their own shadow



His **fingers** are closed around thin air rather than the coffee cup he carries



The **crucifix** is held inexplicably aloft with the other half of the chain missing



interioryesplz



2,168 likes

interioryesplz Sunny kitchen 🌞🍁🌟... more



apartmenttherapy
Morton Grove, Illinois



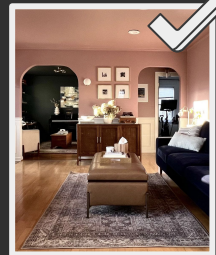
2,353 likes

apartmenttherapy Pro design couple Savannah and Kaitlyn Stone (@ainslie_design_studio) made an all-white living

TWO CLASSES OF IMAGES



WITHOUT
CREDIBLE
METADATA,
ATTESTATIONS,
& SUPPORTING
DOCUMENTS



WITH
CREDIBLE
METADATA,
ATTESTATIONS,
& SUPPORTING
DOCUMENTS

CAN'T AI JUST GENERATE
FAKE DATA TO GO
WITH THE IMAGES?

THERE ARE SOME THINGS
THAT CAN'T BE FAKED

1.

WE CAN MAKE IT
IMPOSSIBLE TO CREDIBLY
BACKDATE AN IMAGE

2.

WE CAN MAKE IT
NEARLY IMPOSSIBLE
TO FAKE SOURCES AND
TAMPER WITH CLAIMS



TIMESTAMPING SERVICE

Submit an image or file, get a proof that the file **existed before a certain point in time.**

"All the News
That's Fit to Print"

The New York Times

THE WEATHER

Today, variably cloudy, windy, cool, high 56. Tonight, mostly cloudy, still windy, low 46. Tomorrow, partly sunny skies, a northwest wind, high 60. Weather map is on Page 24.

VOL. CLXXIII . . . No. 59,949

© 2023 The New York Times Company

SUNDAY, OCTOBER 22, 2023

Prices in Canada may be higher

\$6.00

Israel Is Urged To Avoid a War With Hezbollah

U.S. Warns of Dangers of Widening Conflict

This article is by Edward Wong, Ronen Bergman and Julian E. Barnes.

TEL AVIV — President Biden and his top aides have been urging Israeli leaders against carrying out any major strike against Hezbollah, the powerful militia in Lebanon, that could draw it into the Israel-Hamas war, American and Israeli officials say.

The U.S. officials are concerned that some of the more hawkish members of Israel's war cabinet have wanted to take on Hezbollah even as Israel begins a long conflict against Hamas after the Oct. 7 attacks. The Americans are conveying to the Israelis the difficulties of battling both Hamas in the south and a much more powerful Hezbollah force in the north.

U.S. officials believe Israel would struggle in a two-front war and that such a conflict could draw in both the United States and Iran, the militia's main supporter.

The effort by top American officials to head off an Israeli offensive on Hezbollah, reported in detail here for the first time, reveals anxieties by the Biden administration over the war planning of Prime Minister Benjamin Netanyahu and his aides, even as the two governments strive to present a strong united front in public.

American officials want to rein in Hezbollah too. In numerous meetings across the Middle East, American diplomats have been urging their Arab counterparts to help pass messages to the militia, including via their contacts in Iran, to try to prevent any Israeli

FIRST PART OF AID FLOWS INTO GAZA AT EGYPT BORDER

FOOD, WATER, MEDICINE

Delayed Over Israeli Fear That Weapons Could Be Sent to Hamas

By THOMAS FULLER
and VIVIAN YEE

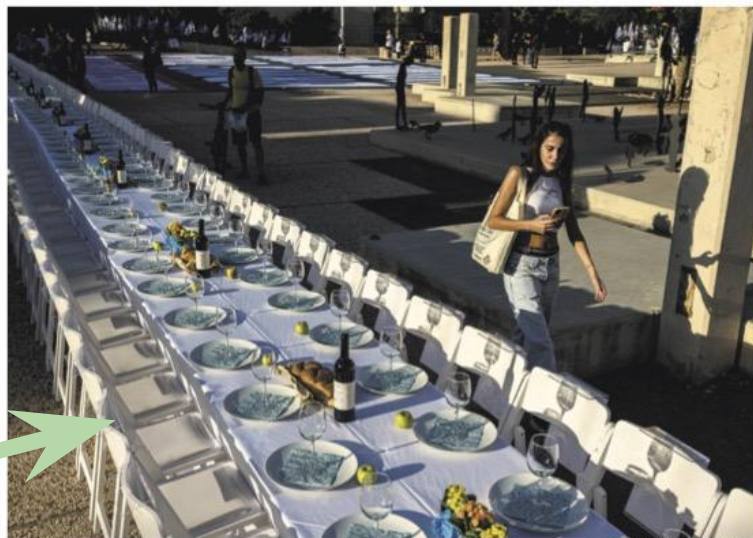
After days of diplomatic wrangling, 20 trucks carrying food, water and medical supplies crossed into Gaza on Saturday, providing a ray of hope for the more than two million residents of the enclave, whose living conditions the United Nations called "catastrophic."

The first of what U.N. officials described as a trickle of aid, a respite in Israel's blanket siege of the enclave imposed after the Hamas terrorist attacks of Oct. 7, came after intense negotiations, including during President Biden's visit to Israel last week.

But the deal allowed the passage of only a fraction of the long line of trucks waiting to carry 3,000 tons of aid from Egypt into Gaza. Negotiations for future shipments were continuing, and it was unclear when more aid would be allowed in.

"The supplies currently heading into Gaza will barely begin to address the escalating health needs as hostilities continue to grow," the World Health Organization, which supplied trauma kits as part of the convoy, said in a statement on Saturday. "Much more is needed."

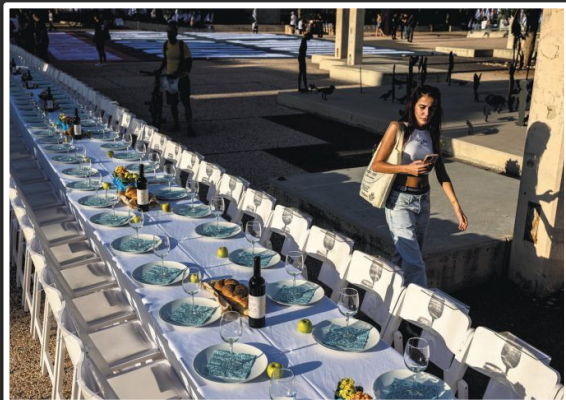
Continued on Page 12



TAMAR KALIFA FOR THE NEW YORK TIMES

Remembering the Missing

In Tel Aviv, 203 place settings, one for each hostage believed to be in Gaza. Worries are growing for the most frail hostages. Page 13.



College Football Now Has Wages Over \$100,000

By DAVID A. FAHRENTHOLD
and BILLY WITZ

The key to recruiting top college football players these days is

Conflicts Further Fueling a Global Arms Rush

By ERIC LIPTON

WASHINGTON — Just days after the assault by Hamas ignited a new war in the Middle East, shipments of American weapons began arriving in Israel: smart bombs, ammunition and interceptors for the Iron Dome missile-defense system. When President Bi-

U.S. Seeks to Bolster Ties, While Keeping Up With Demand

Congress a request for more than \$70 billion in assistance for

the Biden administration with new opportunities to tie the militaries of other countries more closely to the United States, the world's biggest arms exporter, while also raising concerns that a more heavily armed world will be prone to armed into further wars.

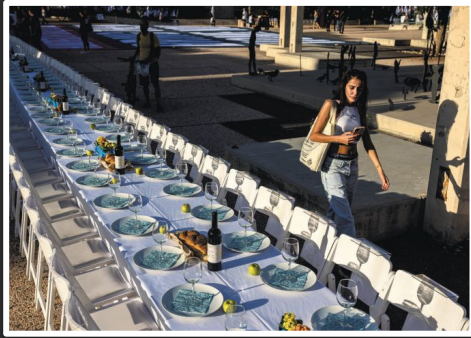
Even before Israel responded to the deadly Hamas attack, the



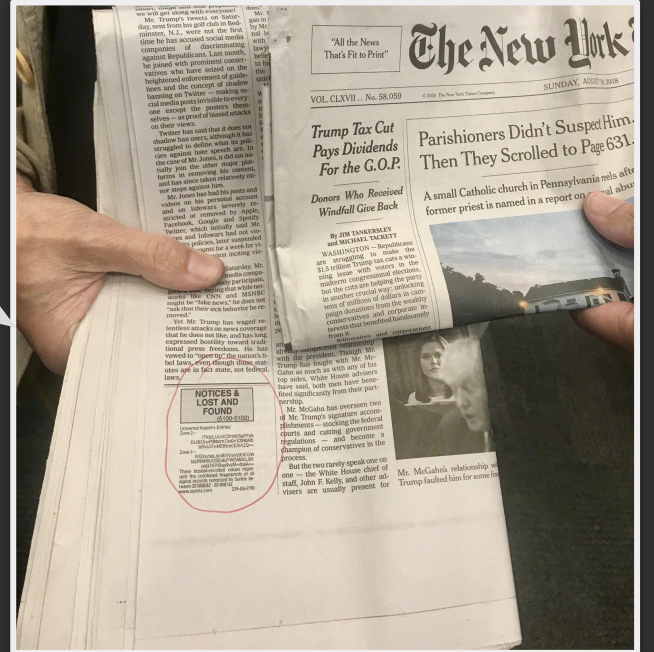
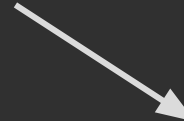


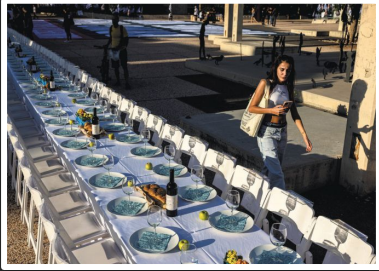
CRYPTOGRAPHIC HASH

A cryptographic hash is a unique identifier derived from the contents.



0xb8668593b
fe1ed03f11b
18db597fc22
1ea505936ad
b0af3beb182
1e0ae0e53b6





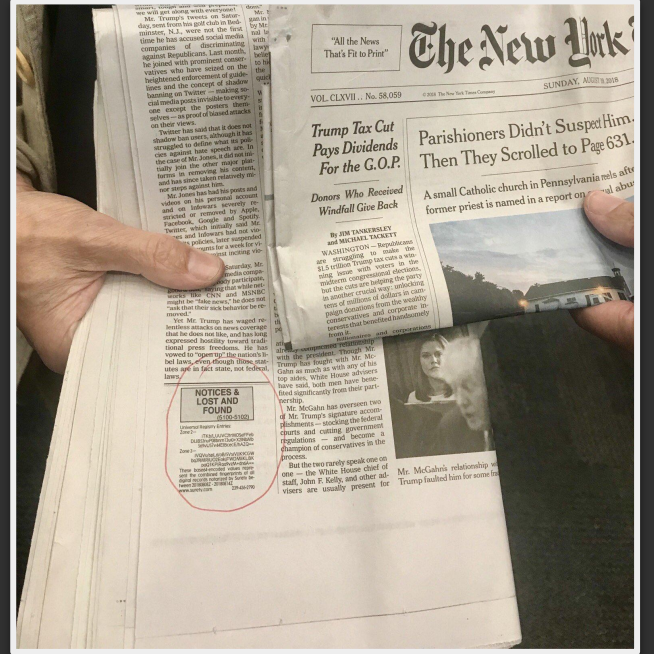
@xb8668593
bfe1ed03f1
1b18db597f
c221ea5059
36adb0af3b
eb1821e0ae
0e53b6

Concatenate
and hash



@xaa9cdfb6
d7c2e93c27
e1a3def29f
738b0bc99c
a9ae8f0b8a
fa7d02c2ef
0612af

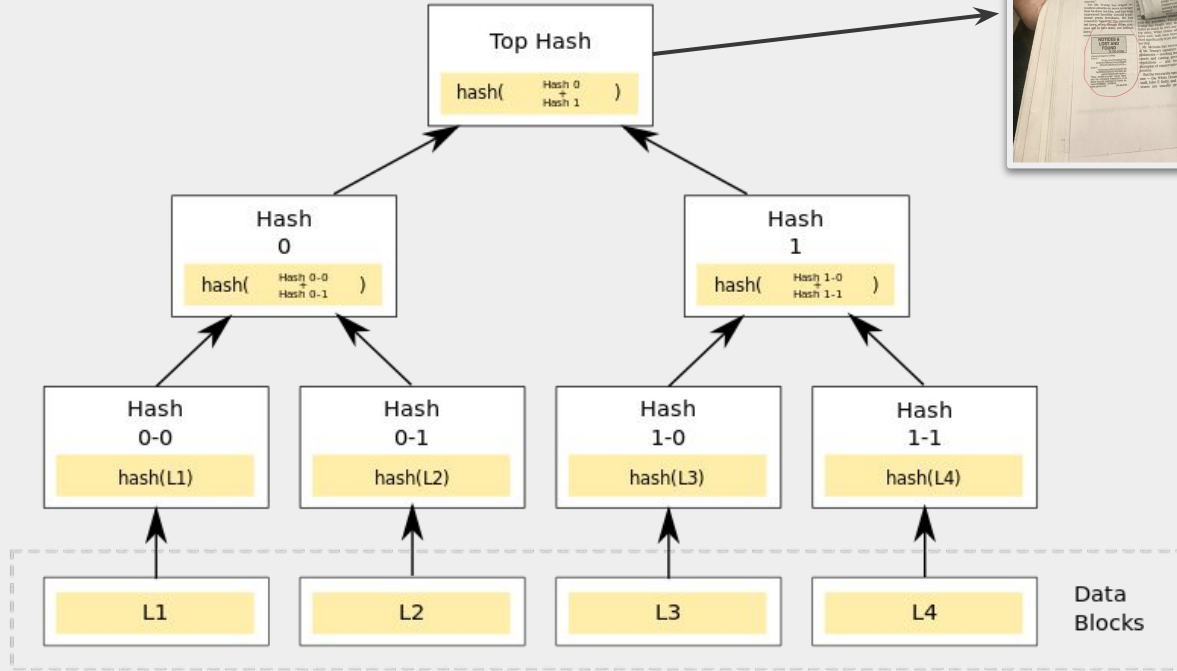
@xb8668593
bfe1ed03f1
1b18db597f
c221ea5059
36adb0af3b
eb1821e0ae
0e53b6



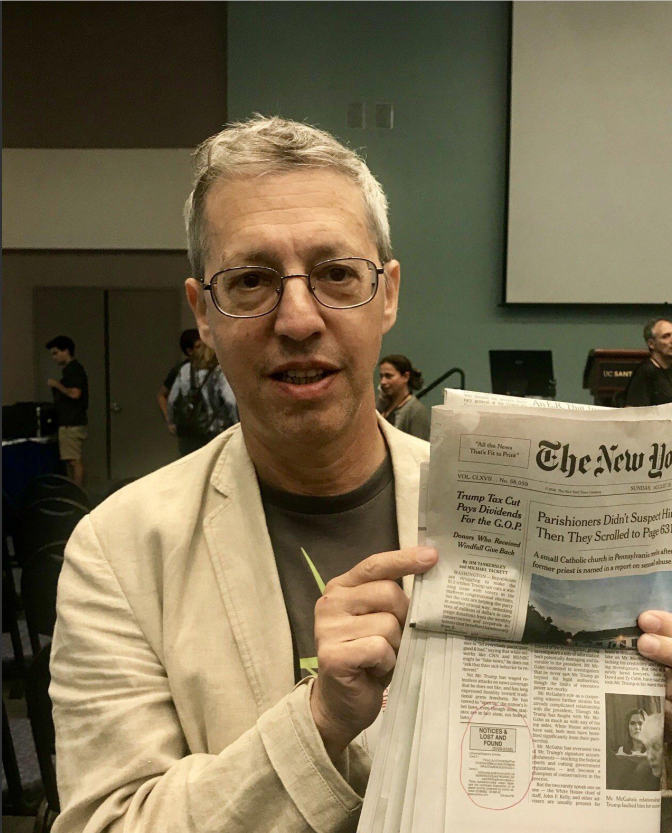
MERKLE TREE



Proof size:
 $O(\log_2 n)$,
roughly the
height of the
binary tree



ANCHORING



vowed to "open up" the nation's libel laws, even though those statutes are in fact state, not federal, laws.

NOTICES & LOST AND FOUND
(5100-5102)

Universal Registry Entries:
Zone 2—

1TKb/LUUVc2trMOSeFFeb
DIJB53nuP08bnrmt3ui0+X2INbMb
569vU57v44EIBccecE/hAZQ

Zone 3—

1VQVv/sPL6/oBj/5VsvI/K9CGW
bq39iMRiU02EokjFwDmiiKLBK
paQ1KPiRqa9vz7M+dn6A

These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 20180808Z - 20180814Z
www.surety.com 239-436-2790

STUART HABER
AUDITCHAIN
UNITED STATES

"All the News That's Fit to Print"

The New York Times
SUNDAY, AUGUST 12, 2018
VOL. CLXXVII, No. 58,059

Trump Tax Cut Pays Dividends For the G.O.P.
Donors Who Received Windfall Give Back

Parishioners Didn't Suspect Then They Scrolled to Page 3
A small Catholic church in Pennsylvania's former priest is named in a report on sexual abuse

By JIM TANKERSLEY and MICHAEL WICKERT
WASHINGTON — Republicans are struggling to make the case that the Trump tax cut is a win-win, even with voters in the middle of congressional elections. But the cuts are helping the party in another crucial way: strengthening its dominance in the wealthy investor and corporate interest world that benefitted handsomely from the administration's policies.

Mr. Trump has waged relentless attacks on news coverage that he does not like, and has long expressed hostility toward traditional print media. The nation's best laws, even though those statutes apply in fact state, not federal, law.

NOTICES & LOST AND FOUND
(5100-5102)

Universal Registry Entries:
Zone 2—
Zone 3—

These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 20180808Z - 20180814Z
www.surety.com 239-436-2790

Mr. McCabe's relationship with Trump faulted him for some time

ANCHORING



2.

WE CAN MAKE IT
(NEARLY) IMPOSSIBLE
TO FAKE SOURCES AND
TAMPER WITH CLAIMS



DIGITAL SIGNATURES

Using cryptography, we can sign a piece of data in a way that can't be forged or repudiated

DIGITAL SIGNATURES ALLOW US
TO SHARE SECONDHAND DATA
AS IF IT CAME DIRECTLY
FROM THE SOURCE

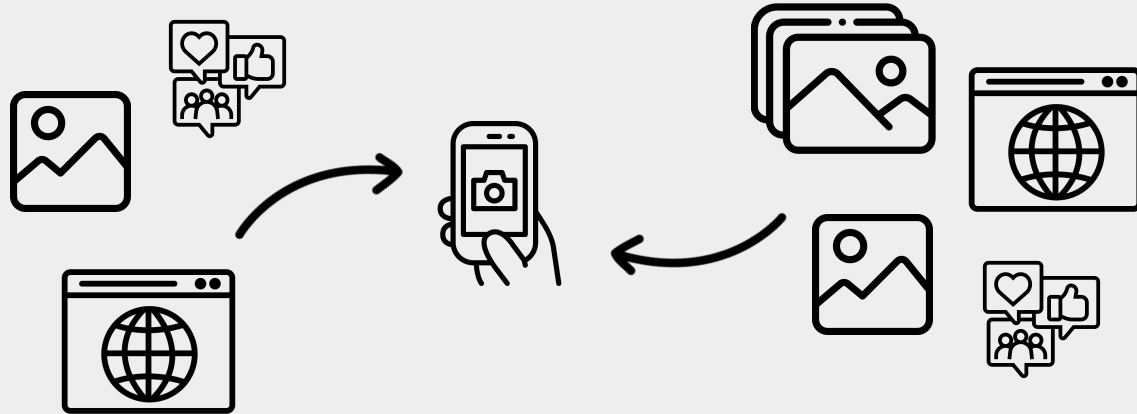
VERIFICATION IS FUZZY AND HUMAN



<https://www.bellingcat.com/resources/case-studies/2015/05/28/geo-locating-stanislav-tarasov/>

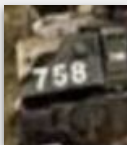
A WEB OF KNOWLEDGE

Investigation requires collecting more and more web pages, images, and other documents. *All related to the original source.*

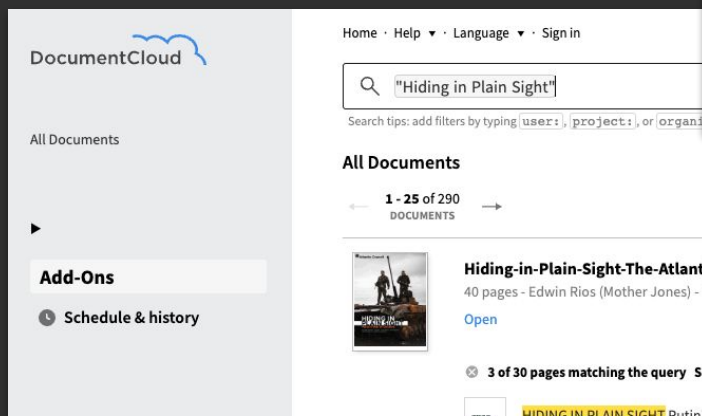
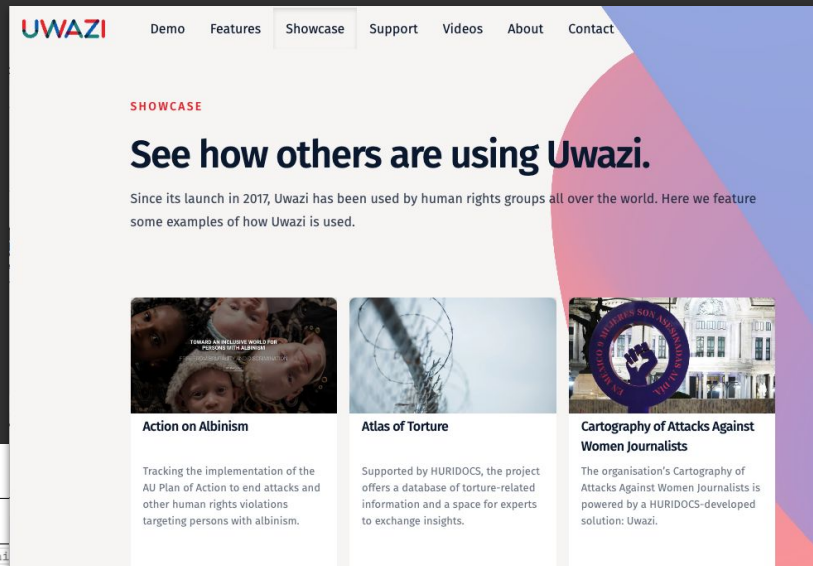
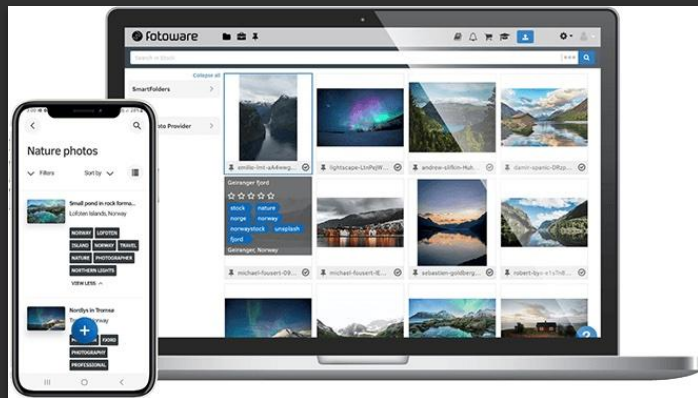


AUTHENTICATED ATTRIBUTES

Making investigations *shareable*



SOFTWARE AND SYSTEMS FOR INVESTIGATION



AUTHENTICATED ATTRIBUTES ARCHITECTURE



Front-end Asset Management System
(Demo: Uwazi)



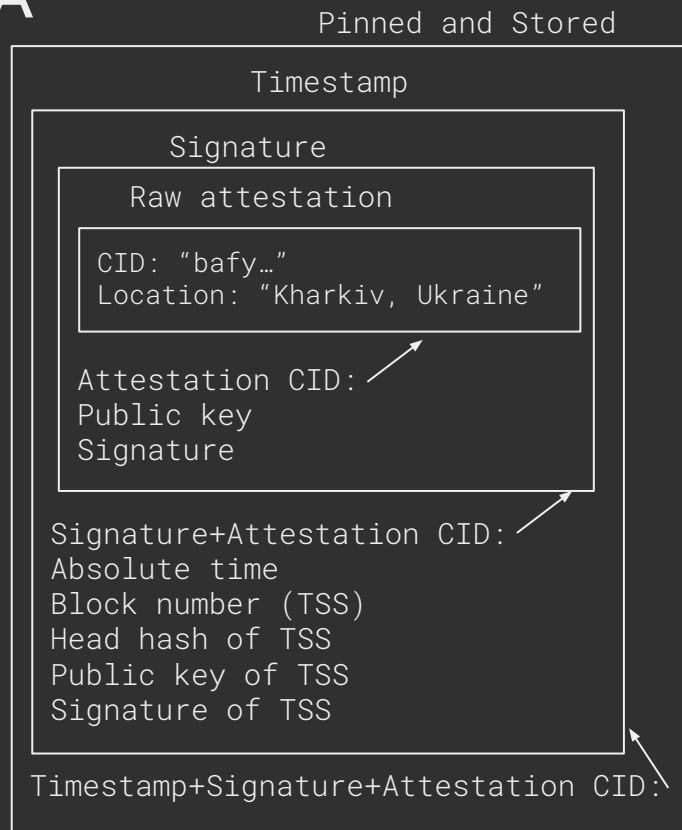
Authenticated Data



Peer-to-Peer Database
(Demo: Hyperbee)

AUTHENTICATED DATA SCHEMA

- All metadata individually signed and timestamped
 - Can be exported individually (e.g. as Verifiable Credentials)
- Cryptographic hash: SHA256 CIDv1
- Storing the data as DAG-CBOR
 - Can store each attribute directly in IPFS
 - Can make comments about attributes/attestations themselves by referencing *their* CID
- Digital Signature library is Noble Crypto (@noble/ed25519)
- Encryption: NaCl JavaScript library (xsalsa20-poly1305)
- Timestamping Service: OpenTimestamps



THANKS!

Any questions?

<https://github.com/starlinglab/authenticated-attributes>

<https://www.starlinglab.org/>

katelynsills@gmail.com

katelynsills.com



AUTHENTICITY-BY-DESIGN
FALL SEMINAR SERIES

Oct 31 **CAPTURE - New Tools to Establish Trust**
Tue 12pm to 1pm | Green Library | Hohbach Hall 122

Nov 7 **STORE - Authenticated Databases**
Tue 12pm to 1pm | Paul G. Allen Center 101X

Nov 30 **VERIFY - Applying Authenticity**
Tue 12pm to 1pm | Packard 204



Join in person at Stanford University -OR- remote on Zoom