**Problem:**

Before an exchange occurs every company, government or institution has to obtain and hold your personal information to validate it is you.

**Current Solution:**

Every company, government or institution has to ask for "two forms of ID", Social Security Number, Utility Bill, Passport and or fill out a form to validate yourself. This costs money and time to obtain this information and to store it securely (or in most cases insecurely).

**Future Solution:**

Offer a service where any company, government or institution can validate anyone's personal information prior to the exchange. The company, government or institution would pay money for temporary access to this validating information for whatever process they are needing to complete.

**How can this occur?:**

Personas

***Owner*** = person that owns their personal information (examples are above - "two forms of ID", Social Security Number, Utility Bill or Passport) that is used to validate who they are.

***Keys*** = the NOSTR (Notes and Other Stuff Transmitted by Relay) protocol allows for the **Owner** to control their personal information through keys as an identification mechanism. There are two keys - 1) npub (nostr public) and 2) nsec (nostr secret). The **Owner's** npub key can be shared with anyone and the **Owner's** nsec key is private and should not be shared (similar to not sharing a password). The **Owner's** npub and nsec keys only work with each other and no other npub and nsec key pair will work.

***Client*** = this is a mobile or desktop application the **Owner** uses to interface and communicate with.

***Relay*** = this is a network of computers that is owned and operated by whomever. This network of computers are "relaying" the **Owner's** **Events** to whomever is requesting it.

***Events*** = An **Event** is any information the **Owner** sends from a **Client** to a **Relay**. When this occurs the **Owner's** **Keys** create a unique signature for the **Event**. This unique signature is like a digital stamp that proves - "Yes, this message really came from the John Smith (**Owner**)." This unique signature can be verified by whomever. This unique signature is created through three actions 1) the **Owner's** “id” (identity) which is the **Owner’s** **Keys**, 2) the “tags” of the **Event** which is hashed and 3) and the “sig” which verifies that the **Owner's** “id” (their **Keys**) is what signed for the **Event**. All three of these mechanism can prove who sent the **Event**, contents of the **Event** and that the **Event** has not been changed or altered.

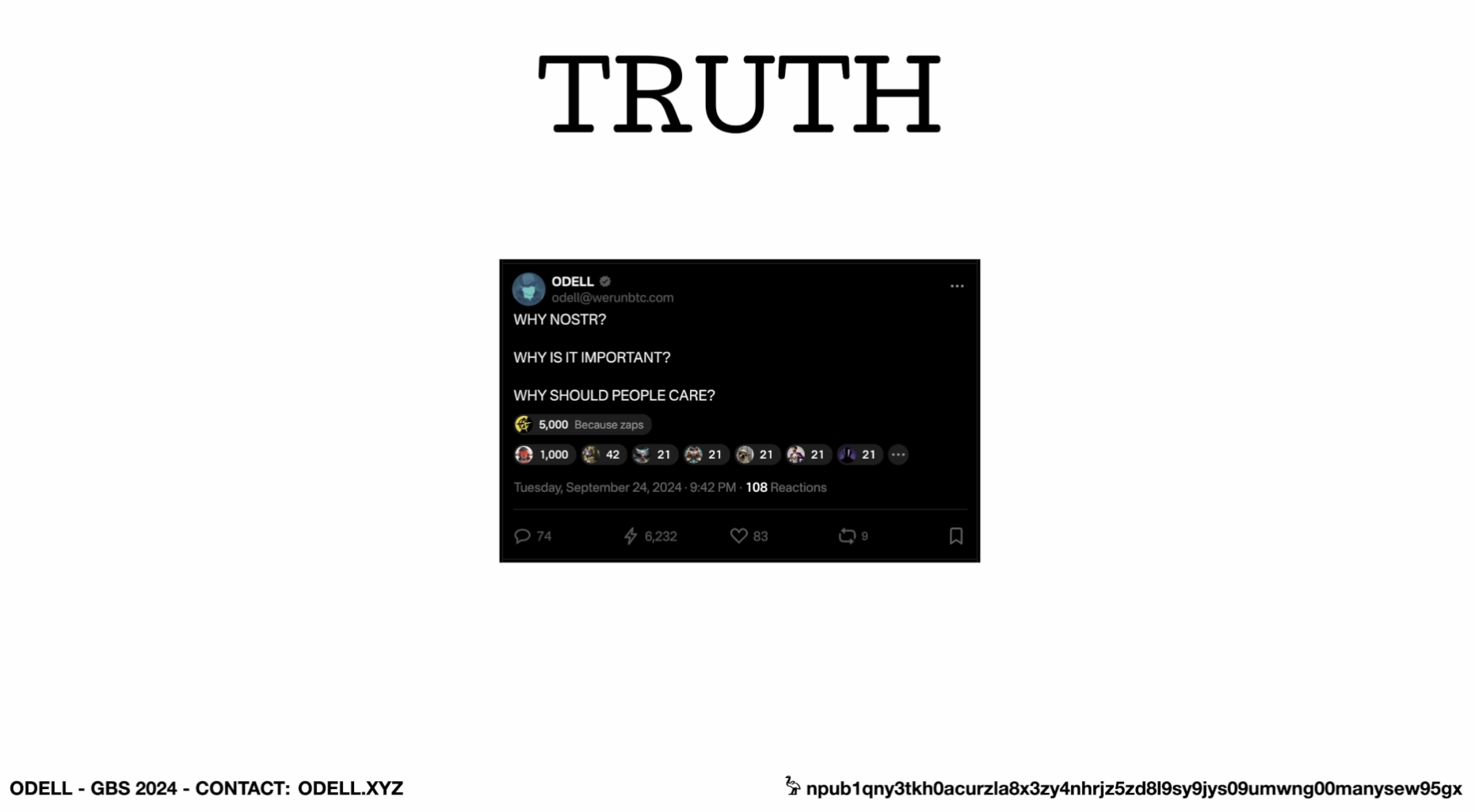
Additional Definitions:

hashed: When the Owner creates an **Event** it is signed with the Owner’s private Key (nsec). This process involves “hashing” the Event’s content. Think of “hashing” as you bake a cookie and give it to someone. They can taste it and say, “Yes, this cookie was made from that specific recipe!” but they can’t figure out the exact ingredients just from eating it. Hashing ensures the integrity and security of the information being sent and verified on the Nostr network.

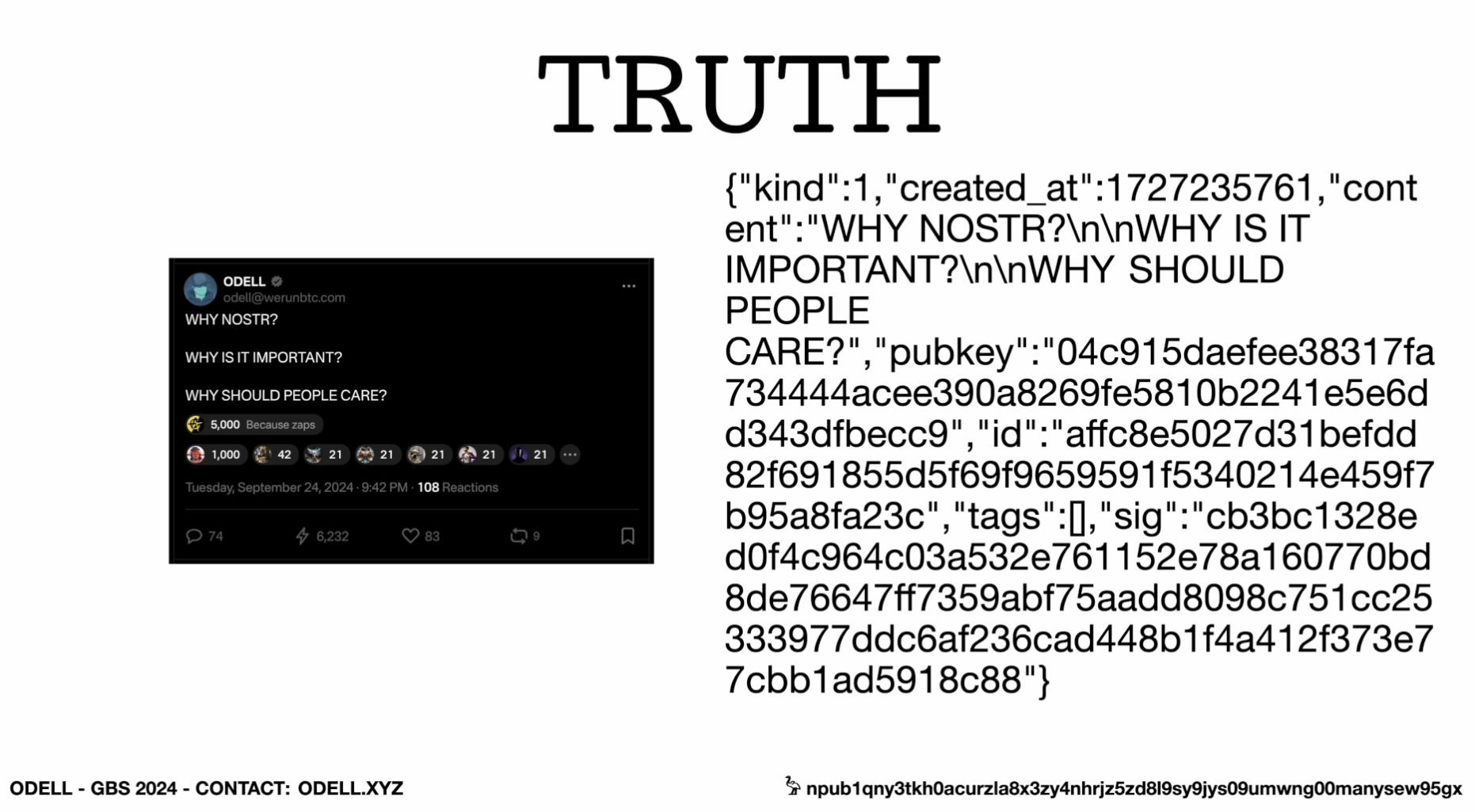
signed for: The proves the Event was created by the Owner of the private key (nsec) that corresponds to the public key (npub).

***Example:***

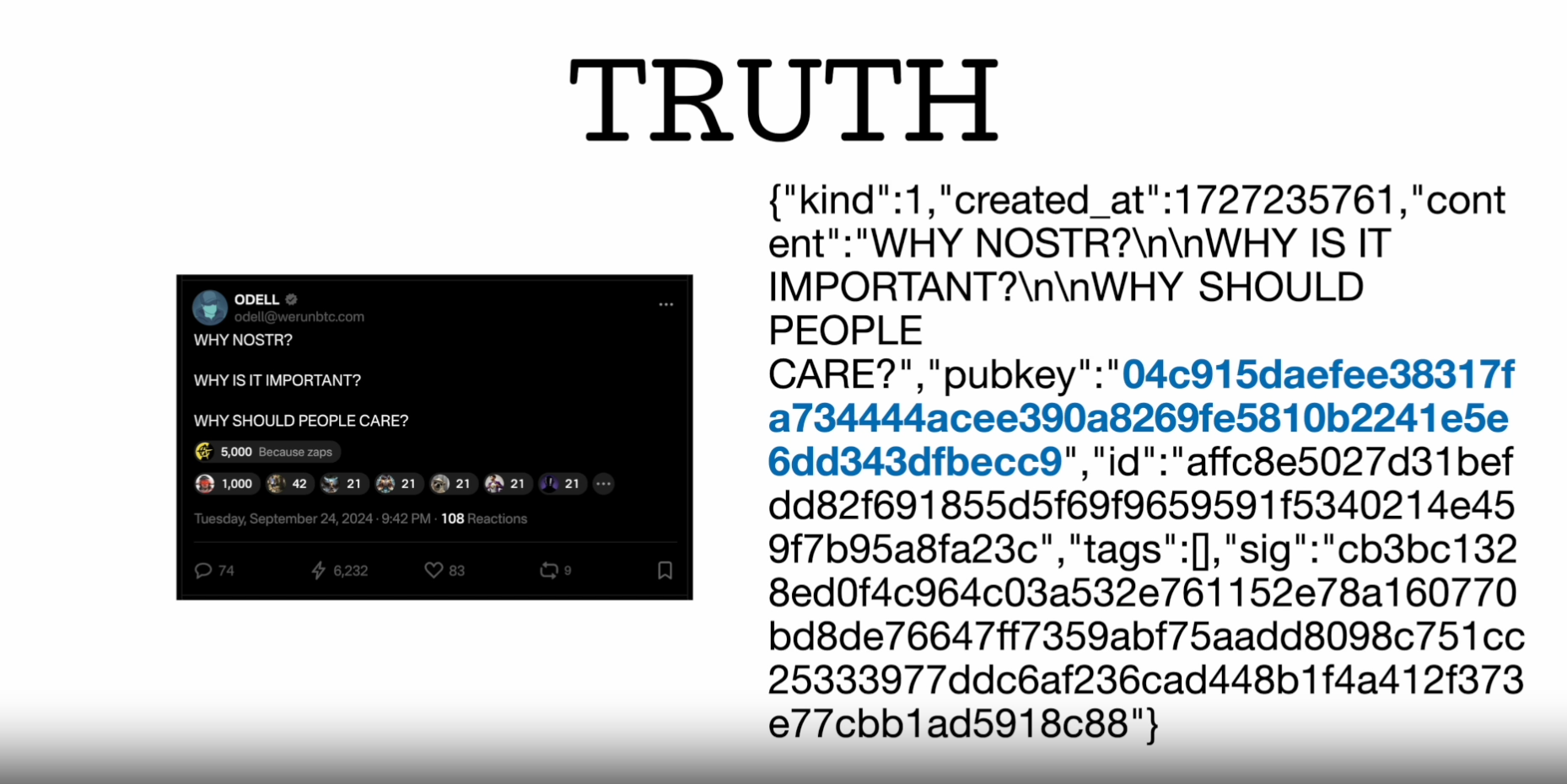
This **Event** was posted on Primal (**Client**) by @ODELL(**Owner**):



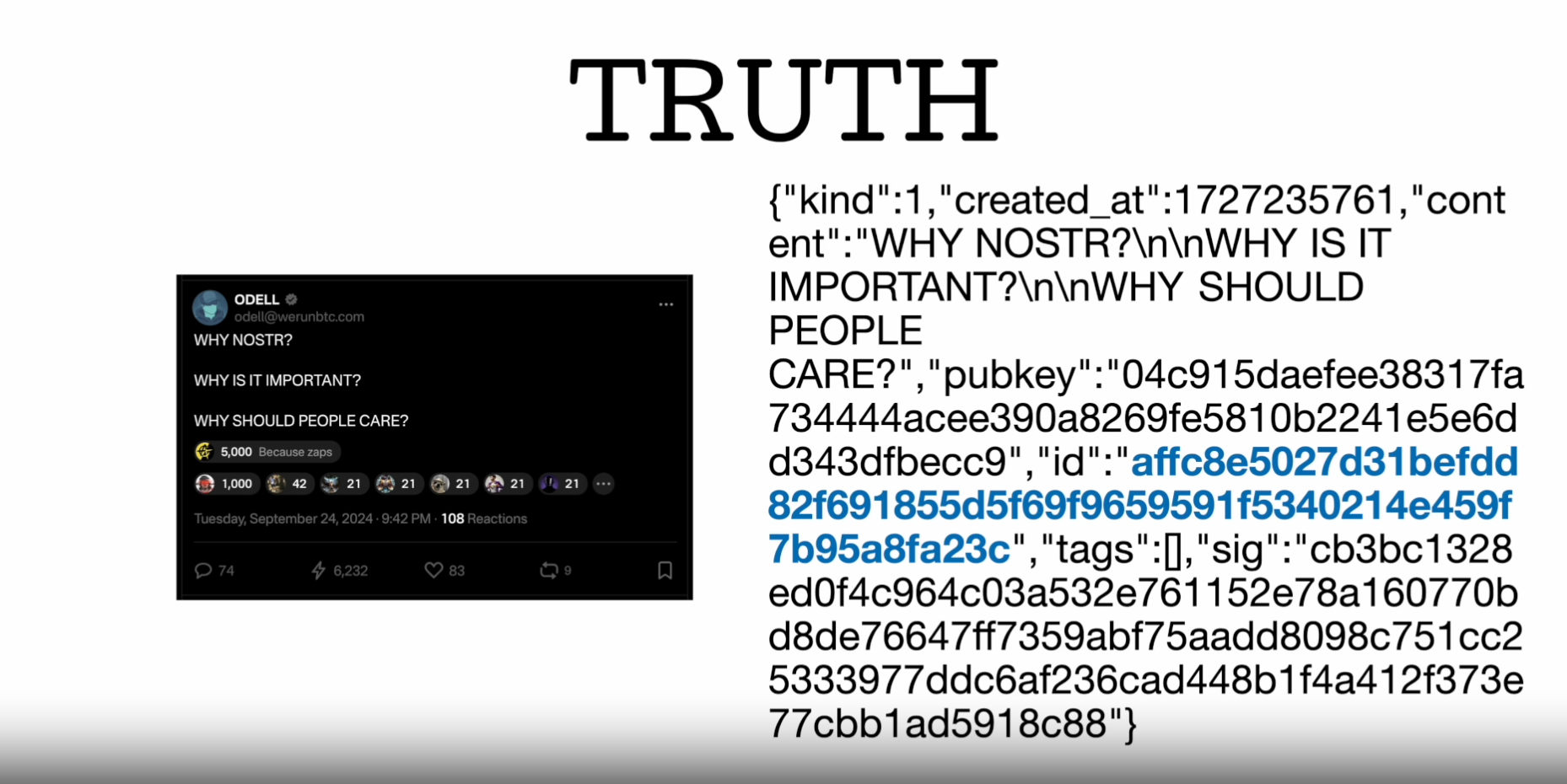
Here are the cryptographic details of this **Event**:



Here is the “id” highlighted in blue:



Here is the “tags” highlighted in blue:



Here is the “sig” highlighted in blue:

We provide a Client. This Client is both a mobile and desktop application. The Client allows for the Owner to provide their personal information - "two forms of ID", Social Security Number, Utility Bill or Passport to any Relay that is requesting it.

The Relay then provides this personal information to the requester (company, government or institution). The requester has to pay the Relay for this information. This payment is then tied to the Relay and the npub of the Owner. So the Owner and the Relay operator will be compensated for providing and storing this personal information.

The requester knows this information is legitimate due to the above process of the NOSTR protocol. The requester also does not have to request (from the Owner) their personal information for verification purposes before an exchange occurs. The requester also does not need to store this personal information in their IT infrastructure which will reduce CapEx, OpEx, Security and Audit related costs and vulnerabilities.