[18.4., 14:24] Yannick Schroth: @Kai bin grade nochmal am whitepaper dran. wie würdest du das auf deutsch neu formulieren mit der neuen technologie?
Antwort:
Wir haben eine Lösung entwickelt, mit der ein unsichtbarer Code direkt in ein Referenzbild eingebettet wird. Dieser Code verweist eindeutig auf das Originalbild. Wird das Referenzbild manipuliert, bleibt die Verknüpfung zum Original bestehen, sodass stets das unverfälschte Bild identifiziert und dem Kunden angezeigt werden kann.

Veraltet:
"A unique, invisible verification code is embedded directly into the image. This code consists of a prefix and a partial hash (e.g., "0-a1b2c3"), creating a tamper-evident seal that travels with the photo."

[18.4., 14:25] Yannick Schroth: und das hier stimmt so nicht, oder? "The hash is stored securely on our servers. Importantly, only the hash is stored. The original image cannot be reconstructed from it, ensuring full GDPR compliance and enabling immediate, permanent deletion when required."
Antwort:
Der Hashwert wird auf der Blockchain gespeichert. Über ihn kann die jeweilige Transaktion gefunden werden, in der auch Metadaten wie Geostandort und Aufnahmezeit hinterlegt sind. Zudem referenziert der Hashwert auf der Blockchain den Hash des Originalbildes.
Der Vorteil liegt in der DSGVO-Konformität, da der Hashwert mathematisch nicht zurückgerechnet werden kann und nur ein grober Standort verwendet wird. Auch das Datum gilt nicht als DSGVO-relevant. Gleichzeitig wird die Datenintegrität durch die Blockchain gewährleistet.

[18.4., 14:25] Yannick Schroth: und das fällt jetzt weg, oder? "Anyone can verify a photo's authenticity by entering the 6-digit code on our web app or through API integration. If the image has been altered in any way, verification fails instantly."
Antwort:
Die Echtheit kann auf 2 Verschiedene Arten festgestellt:
1. Art (Technisch) Originalbild mit einem öffentlich zugänglichen SHA-256-Generator berechnen. Über diesen Hash kann auf unserem Smart Contract auf der Blockchain die Transaktion anhand des Hashwerts gefunden und die Metadaten ausgelesen werden.

2. Gängig: Referenzbild, das den unsichtbaren Code beinhaltet, über die Plattform hochladen. Hierbei wird der Code automatisiert ausgelesen und das Originalbild mit den Metadaten angezeigt.

[18.4., 14:26] Yannick Schroth: stimmt das hier noch? "Change just one pixel, adjust the brightness by 1%, or crop a single millimeter, and the entire hash changes completely."
Antwort:
Ja, das stimmt. Allerdings ist das nur eine allgemeine Beschreibung, wie die Hashwertberechnung funktioniert. Im Umkehrschluss bedeutet das, dass selbst wir als Unternehmen keine Möglichkeit haben, das auf unserem Server gespeicherte Originalbild zu ändern, ohne dass es bei der Verifizierung durch den Kunden auffallen würde.

[18.4., 14:27] Yannick Schroth: das hier stimmt so auch nicht, oder? "Many verification systems rely on blockchain or IPFS. These technologies are designed for permanence. But permanence is the enemy of privacy. When users have the right to be forgotten, immutable storage becomes a liability. TrustCamera takes a different approach. We store only the cryptographic hash, never the image itself. This hash cannot be reversed to reconstruct the original photo. It's a one-way proof that the image existed in a specific form, nothing more."
```

Antwort: Ne das stimmt nicht mehr. das kannst du wegmachen.
```