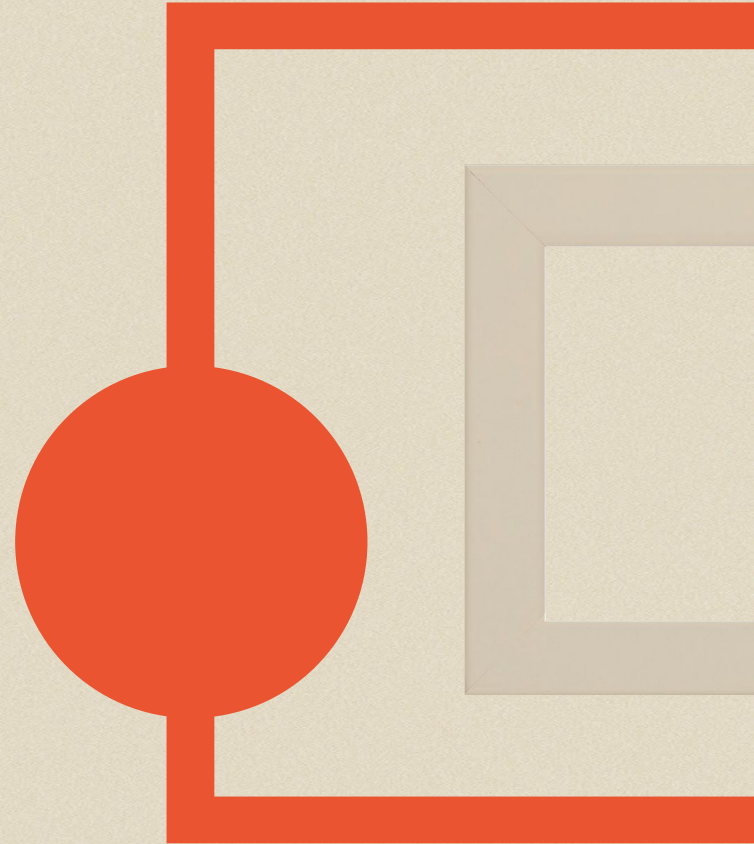


Tamper-Evident Logs and Unalterable Documents

Kate Sills

2022 Foresight Crypto, Security &
AI Workshop





THE MISSING PRODUCTS

COSTLY PROBLEMS IN THE “REAL WORLD”



- Need to prevent fraud & other malicious behavior
- Current solutions:
 - Controls
 - Auditing
 - Machine learning for fraud detection

THE PRODUCTS



POWERFUL CRYPTOGRAPHIC TOOLS



- Hashes
- Digital Signatures
- Hash pointers

For more info:

Fossandcrafts.org Episode 45
Intro to Cryptography

THE MISSING PRODUCTS



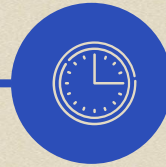
UNALTERABLE DOCUMENTS

Can easily detect even the smallest changes to a document



UNFORGEABLE SIGNATURES

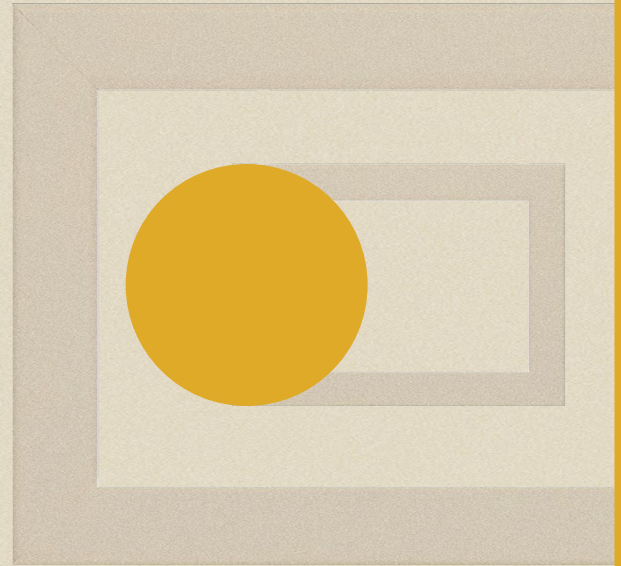
Can easily verify that a document was signed by someone



TIMESTAMPED RECORDS

Can prove that a document existed in a certain point in time

WHY AREN'T
WE USING THE
CRYPTOGRAPHIC
TOOLS?





Why aren't we using the cryptographic tools?

1. In many cases, we are, and we don't realize it!
2. There's a cultural disconnect between cryptographers (mathematicians) and the people that need the solutions (businesspeople)
3. Cryptographers aren't generally known for good UX design (sorry!)
 - a. Why Johnny Can't Encrypt (Whitten 1999)
4. Confusion about blockchains
 - a. Bitcoin didn't invent hashes, digital signatures, or "blockchains"
 - b. Timestamping Service with Tamper-evident Logs (Haber & Stornetta 1991)

TIME-STAMPING SERVICE

**USERS PAY WITH
CREDIT CARD**

**USER SUBMITS
DOC HASH TO
SERVICE**

**SERVICE ADDS
HASH TO
“BLOCKCHAIN”**

**SERVICE SENDS
BACK A
DIGITALLY
SIGNED RECEIPT**

**SERVICE
REGULARLY
PUBLISHES HASH
AT HEAD OF
CHAIN**

**USER CAN
PROVE DOC WAS
CREATED
BEFORE A
CERTAIN TIME**

CENTRALIZED TIME-STAMPING

...IS FINE

SAFETY

- SIGNED RECEIPTS
- COPY OF CHAIN
- REGULAR PUBLICATION OF HASH AT HEAD OF CHAIN (NEWSPAPER, OTHER BLOCKCHAIN)

LIVENESS

- WORST CASE: DROPS REQUESTS OR SHUTS DOWN ENTIRELY
 - CAN JUST SWITCH TO A COMPETITOR, SINCE NO VALUE IS LOCKED UP ON-CHAIN

TAKEAWAY

**DECENTRALIZED
BLOCKCHAINS
ARE COSTLY**

**CRYPTOGRAPHIC
TOOLS
ARE CHEAP**





THANKS!

katelynsills@gmail.com
[@kate_sills](https://www.instagram.com/kate_sills)
katelynsills.com

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, infographics & images by Freepik and illustrations by Storyset