Steganography & Real-World Cryptography

“It’s not just what you encrypt - it’s where you hide it.”

CЯ4CK1NG-THΞ-C0D3

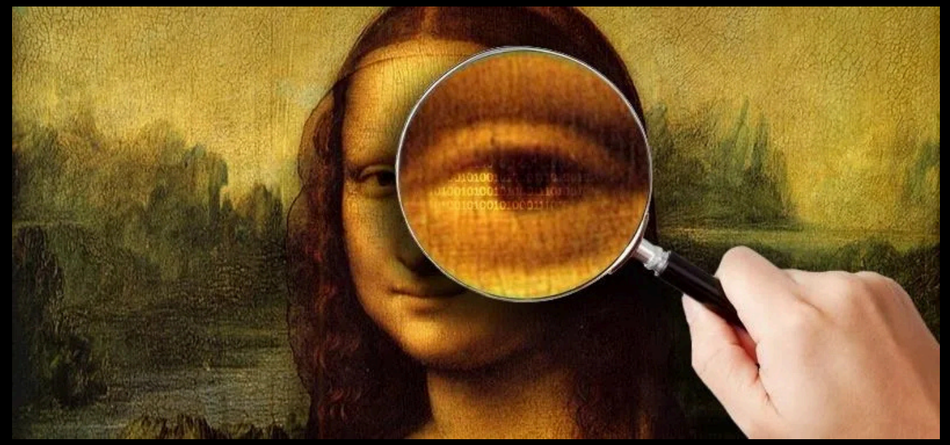
Today’s Roadmap

- The Art of Hiding: Steganography
- Tools & Techniques (Hands-On)
- Secrets in the Wild – Real-World Encryption
- E2EE & Blockchain

Lets start off with Steganography

What is Steganography?

- From Greek steganos (hidden) + graphein (writing).
- It’s not encryption, but concealment — hiding information within other media.
- Examples:
  - Text hidden inside an image.
  - Audio files with embedded data.
  - Invisible messages in HTML or metadata.



Steganography vs Cryptography

Cryptography
Hides the *content* of a message
Visible ciphertext (looks scrambled)
Detectable but unreadable
Example: Caesar Cipher, AES

Steganography
Hides the *existence* of a message
Invisible data inside normal files
Undetectable unless analyzed
Example: Steghide, Invisible Ink

How does it work?

Image Steganography

- Hiding the data by taking the cover object as the image is known as image steganography.
- A digital image is a grid of tiny dots called pixels.
- Each pixel represents color intensity for Red, Green, and Blue (RGB) components.
- These intensities are stored as binary numbers (usually 8 bits per channel).

Example (24-bit RGB image):

- Each pixel = 3 bytes = 24 bits

→ 8 bits for Red, 8 for Green, 8 for Blue

→ e.g., (R,G,B) = (10110110, 11001000, 11110010)

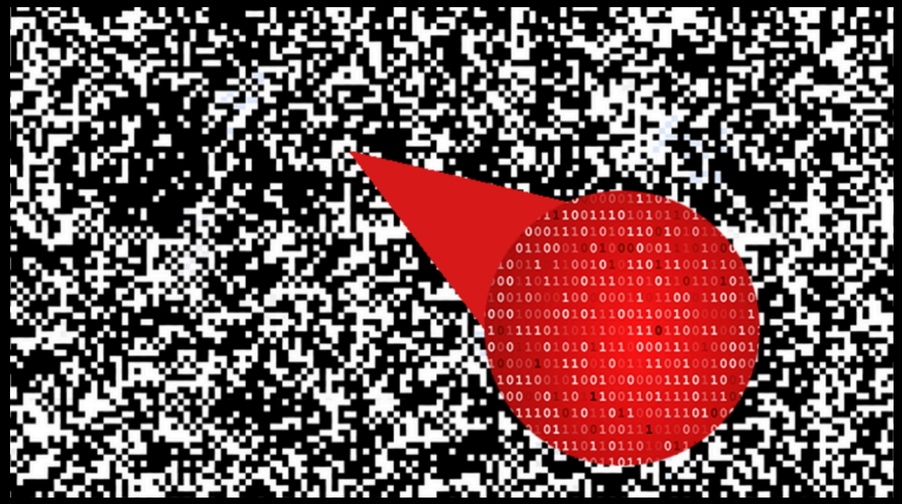


Image Steganography

Least Significant Bit (LSB) Insertion

→ Hides data by replacing the least significant bits of pixel values, causing invisible color changes.

Masking and Filtering

→ Embeds data by slightly adjusting brightness or color in visually insignificant regions like textures or shadows.

Redundant Pattern Encoding

→ Conceals information through repeated or structured patterns that look natural but carry hidden data.

Encrypt and Scatter

→ Encrypts the message first, then randomly scatters encrypted bits across the image using a secret key.

Coding and Cosine Transformation (DCT Method)

→ Hides data in the frequency domain by modifying discrete cosine transform coefficients instead of raw pixels.

Text Steganography

- Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts.
- Various techniques used to hide the data in the text are:
  - Format Based Method
  - Random and Statistical Generation
  - Linguistic Method

Audio Steganography

In audio steganography, the secret message is embedded into an audio signal which alters the binary sequence of the corresponding audio file.
Different methods of audio steganography include:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding
- Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files.

Video Steganography

In Video Steganography you can hide kind of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds. You can think of this as the combination of Image Steganography and Audio Steganography. Two main classes of Video Steganography include:

- Embedding data in uncompressed raw video and compressing it later
- Embedding data directly into the compressed data stream

Lets do a demo

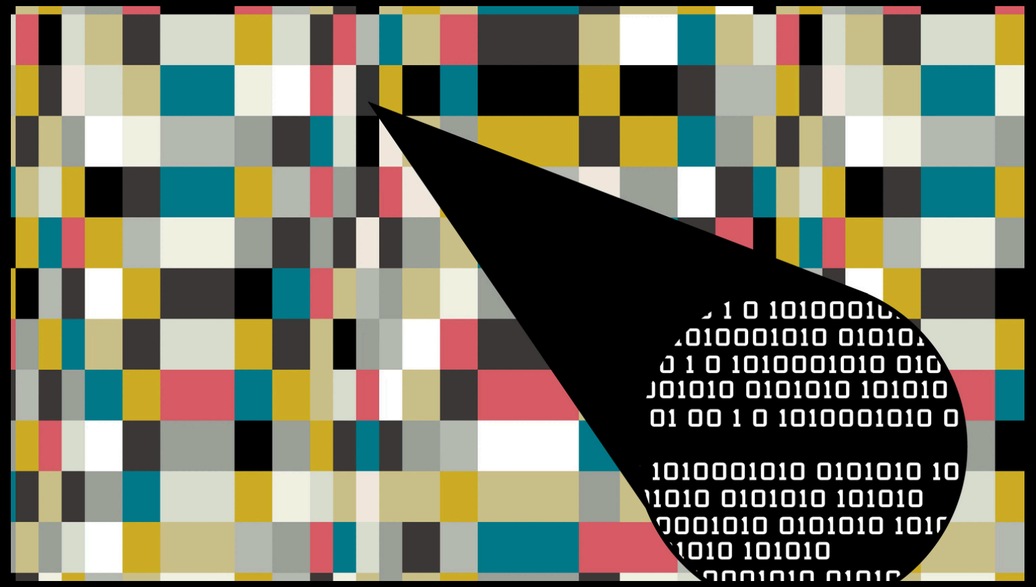
Run this

steghide embed -cf photo.jpg -ef secret.txt -sf hidden.jpg
steghide extract -sf hidden.jpg

Where is useful?

Real-World Use Cases

- Digital Watermarking: Hidden ownership info in images, music, videos.
- Covert Communication: Used by journalists, activists — and sometimes cybercriminals.
- Malware C2 Channels: Attackers hide instructions or payloads in media files.
- Puzzles & ARGs: Cicada 3301 used layered stego to hide cryptographic clues.



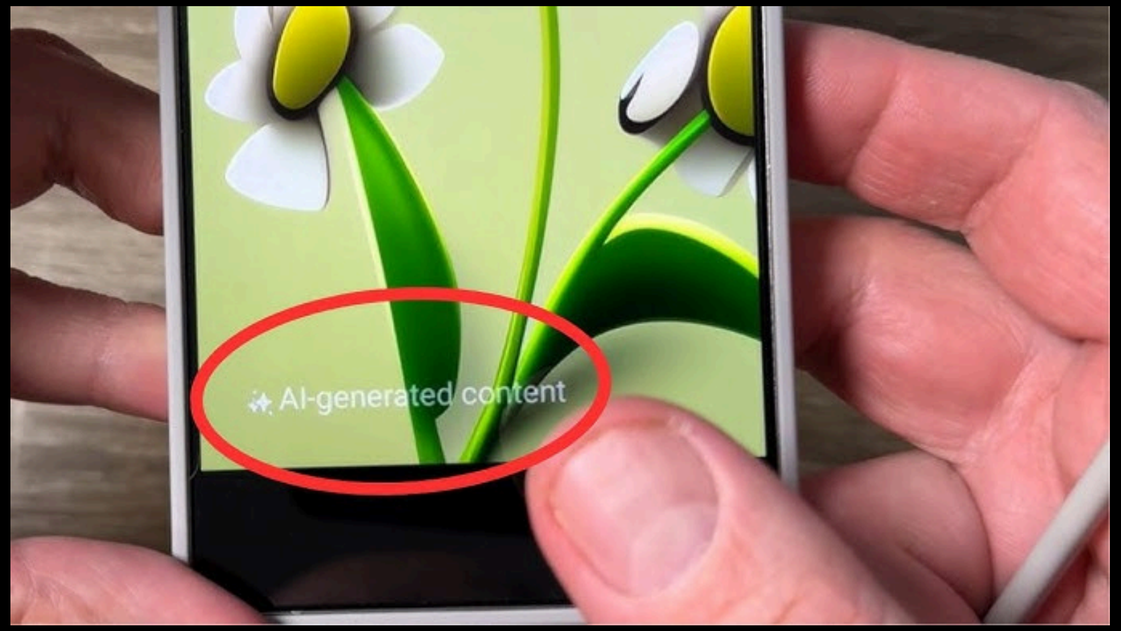
Lets explore one example -

Digital watermarking

- Digital watermarking embeds hidden ownership or authenticity data inside digital media — without visibly altering it.
- Unlike steganography, which hides secret messages, watermarking protects intellectual property.
- It can be visible (logos on stock images) or invisible (bits embedded in pixel/audio data).
- Used for copyright protection, media tracking, and document verification — it’s the digital equivalent of signing your work in code.

- 💡 Steganography hides secrets. Watermarking proves truth.

Modified by Clean Up



Cicada 3301: The Legend

- In 2012, mysterious posts appeared on 4chan:
  - “We are looking for highly intelligent individuals. To find them, we have devised a test.”
- Each clue led to steganographic images, ciphers, coordinates, and cryptographic keys.
  - Solvers used:
  - Image metadata analysis
  - Hash lookups (SHA1/SHA256)
  - PGP key decoding
  - Real-world QR codes in physical locations
- Lesson: Cicada 3301 demonstrated how cryptography, steganography, and real-world investigation intertwine — the ultimate OSINT-meets-crypto puzzle.

The Beginning: The First Cicada 3301 Puzzle

One of the first images to appear as part of the Cicada cypher in 2012

Source: Uncovering Cicada Wiki

On January 4, 2012, an anonymous black-and-white image appeared on 4chan's /b/ message board with the following text:

> *Hello. We are looking for highly intelligent individuals. To find them, we have devised a test...*

Those who recognized the image as a **steganographic puzzle** (a technique used to hide messages within digital images) quickly extracted a string of text leading to a URL. This link revealed the next step in the puzzle, marking the beginning of one of the most sophisticated internet riddles in history.

As participants delved deeper, they encountered a variety of challenges requiring expertise in:

Display a menu

- **Cryptography** (Caesar ciphers, RSA encryption, prime number sequences).

Hello. We are looking for highly intelligent individuals. To find them, we have devised a test.

There is a message hidden in this image.

Find it, and it will lead you on the road to finding us. We look forward to meeting the few that will make it all the way through.

Good luck.

3301

Can you catch a steganographer?

Detecting Hidden Data

- Look for:
  - Unusual file sizes (image looks small but file size is huge)
  - Metadata anomalies (extra EXIF data or edited timestamps)
  - Noise patterns (visual or frequency distortions)
  - Tool signatures (Steghide adds identifiable headers)

```
Last login: Mon Nov  3 09:34:08 on ttys023
pranavhemanth@Pranavs-MacBook-Pro-M3 ~ %cd Downloads
pranavhemanth@Pranavs-MacBook-Pro-M3 Downloads %exiftool letter.png
ExifTool Version Number         : 13.36
File Name                       : letter.png
Directory                       : .
File Size                       : 1292 kB
File Modification Date/Time     : 2025:10:30 22:35:50+05:30
File Access Date/Time           : 2025:11:03 20:58:11+05:30
File Inode Change Date/Time     : 2025:10:30 22:36:05+05:30
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1131
Image Height                    : 1600
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Author                          : Celeste Giverny
Exif Byte Order                 : Big-endian (Motorola, MM)
Y Cb Cr Positioning             : Centered
Exif Version                    : 0232
Components Configuration        : Y, Cb, Cr, -
Color Space                     : Uncalibrated
Image Unique ID                 : ChIJw_Ec9wBy5kcRnKvnOALqti4
Image Size                      : 1131x1600
Megapixels                      : 1.8
pranavhemanth@Pranavs-MacBook-Pro-M3 Downloads %
```

Pros and Cons

- Strengths:
  - Invisible to casual inspection
  - Can bypass basic filters or firewalls
  - Enhances privacy for journalists or whistleblowers
- Weaknesses:
  - Fragile under compression or resizing
  - Low data capacity
  - Once discovered, message security collapses
- Analogy: “Steganography is like hiding a note under your doormat. If no one looks, it’s safe — but if they do, it’s over.”

Challenge Description:

It started with a letter,
A memory of a place.
A public-facing story,
A smile upon her face.
The photo holds the secret,
But the lock is strong and true.
The key is in the music,
Hidden in plain view.
~ Céleste G

Find the trail. Find the key. Find the flag.

Mon cher Toussaint,

Mon cœur retourne si souvent à ce soir de septembre 2014. Paris brillait, comme si elle savait que notre histoire commençait. Je te revois m'attendre à la sortie du Métro.

Ce petit cinéma... J'ai oublié le film, car mon monde entier était la chaleur de ton bras contre le mien. Je suis rentrée cette nuit-là pour écrire toute cette magie sur mon blog. T'es-tu jamais demandé si tu l'avais lu ?

Et ce bistro, où les heures ont fondu en partageant un kir. J'ai su à cet instant que c'était le dernier premier rendez-vous de ma vie.

Cette nuit est notre image parfaite, un moment à nous. Alors, j'ai glissé un petit secret dans celle-ci, juste pour toi. Pense à cette lettre comme à cette belle image... mais ma vraie surprise, mon chéri, est cachée dans son cadre même. Je me demande si tu vas la trouver.

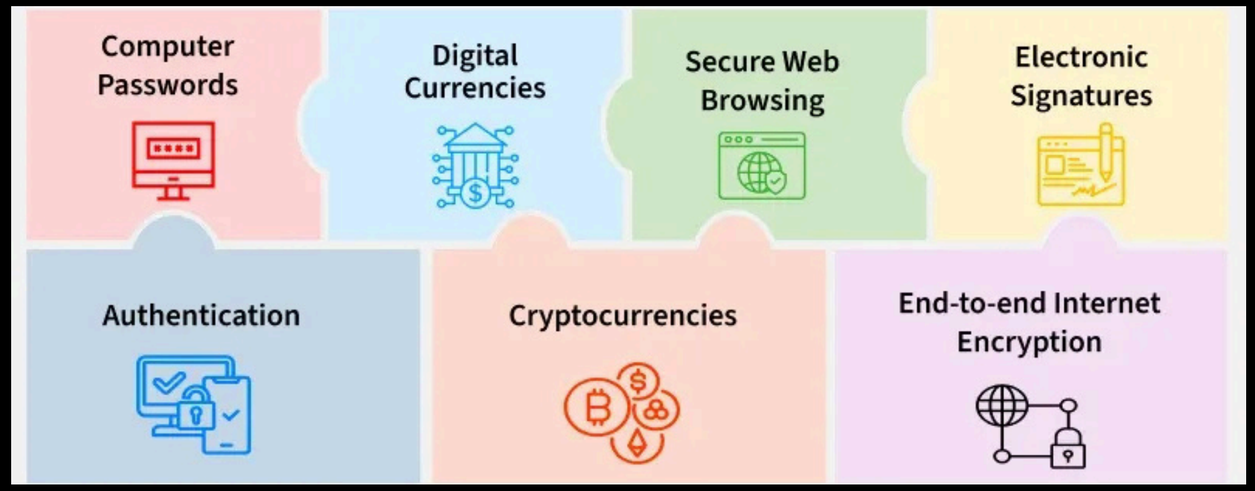
Pour toujours, à toi,

Céleste Giverny

Now lets see Real-World Cryptography

Modern Cryptography in Everyday Life

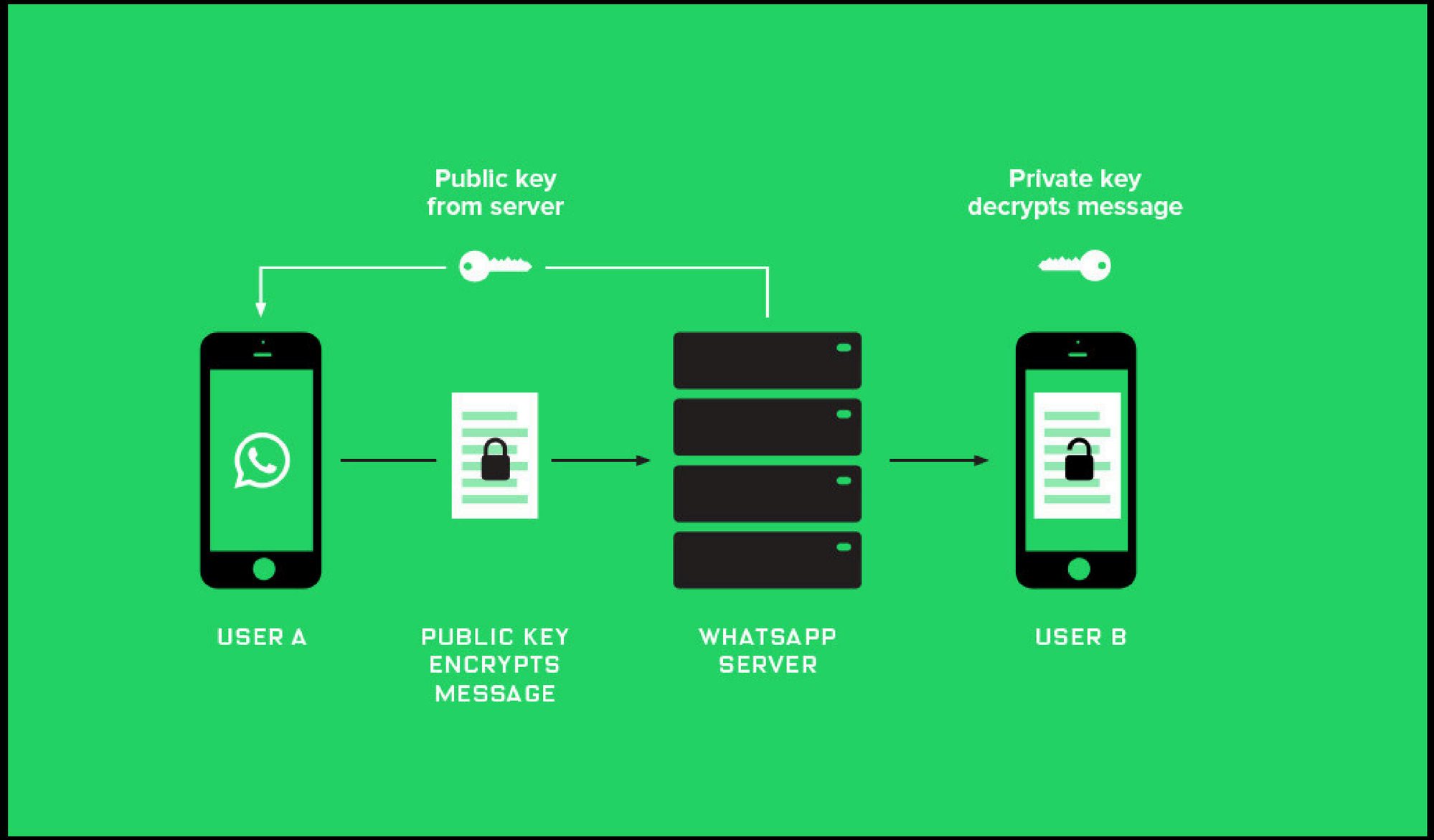
- Cryptography is everywhere — but invisible:
  - Messaging apps: End-to-End Encryption (E2EE) in WhatsApp, Signal
  - Web security: HTTPS / SSL / TLS certificates
  - Finance: Blockchain, digital wallets, cryptocurrencies
  - Auth & Identity: Digital signatures, secure logins



Lets explore one of them

How End-to-End Encryption (E2EE) Works

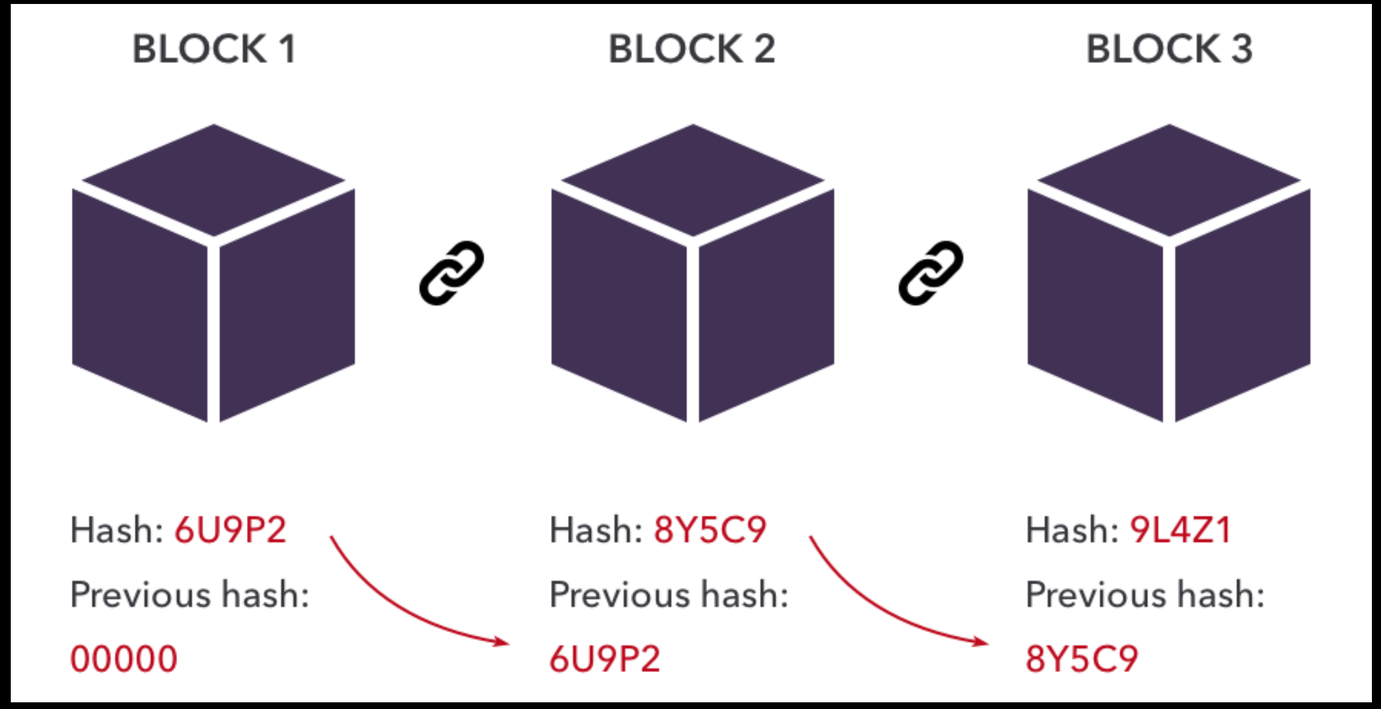
- Alice wants to send Bob a message.
- Alice encrypts with Bob’s public key + her private key (shared key).
- Message travels through server — unreadable to anyone else.
- Bob decrypts with his private key + Alice’s public key.
- Even WhatsApp/Signal servers can’t read the message.
- This shared key is generated every time a new message is sent


Public key
from server
Private key
decrypts message
USER A
PUBLIC KEY
ENCRYPTS
MESSAGE
WHATSAPP
SERVER
USER B

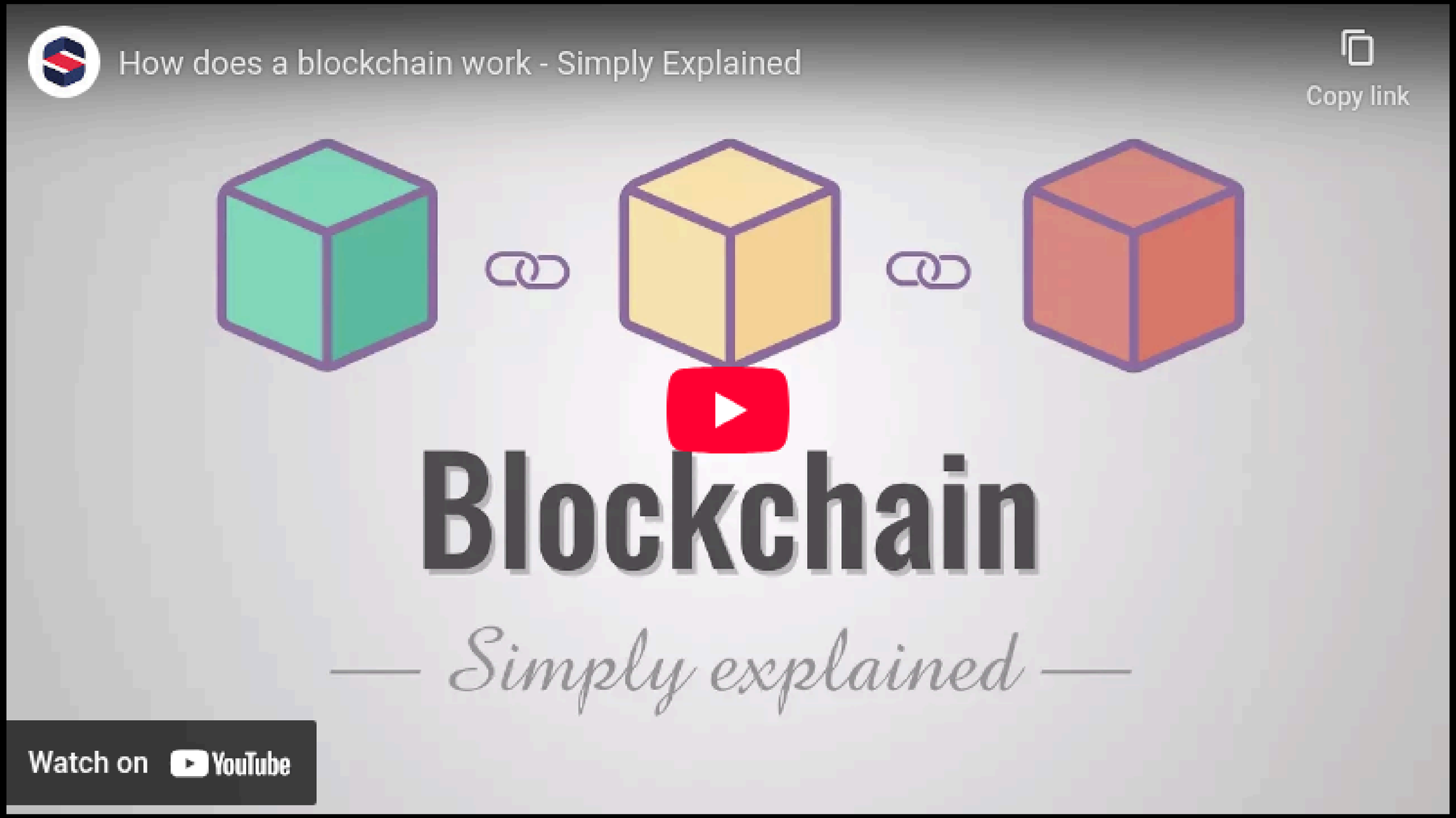
Another modern application very relavant today-

Hashes in the Real World

- Software package verification (apt, npm).
- Blockchain uses hashing for blocks.
- Password storage (but with extra precautions).



remember this slide?


How does a blockchain work - Simply Explained
Copy link
Blockchain
— Simply explained —
Watch on YouTube

Blockchain: Trust Without a Middleman

Concept:

A blockchain is a distributed ledger — no central authority, every node verifies data.

Each block contains:

- **Transactions**
- **Hash of previous block**
- **Timestamp & nonce**

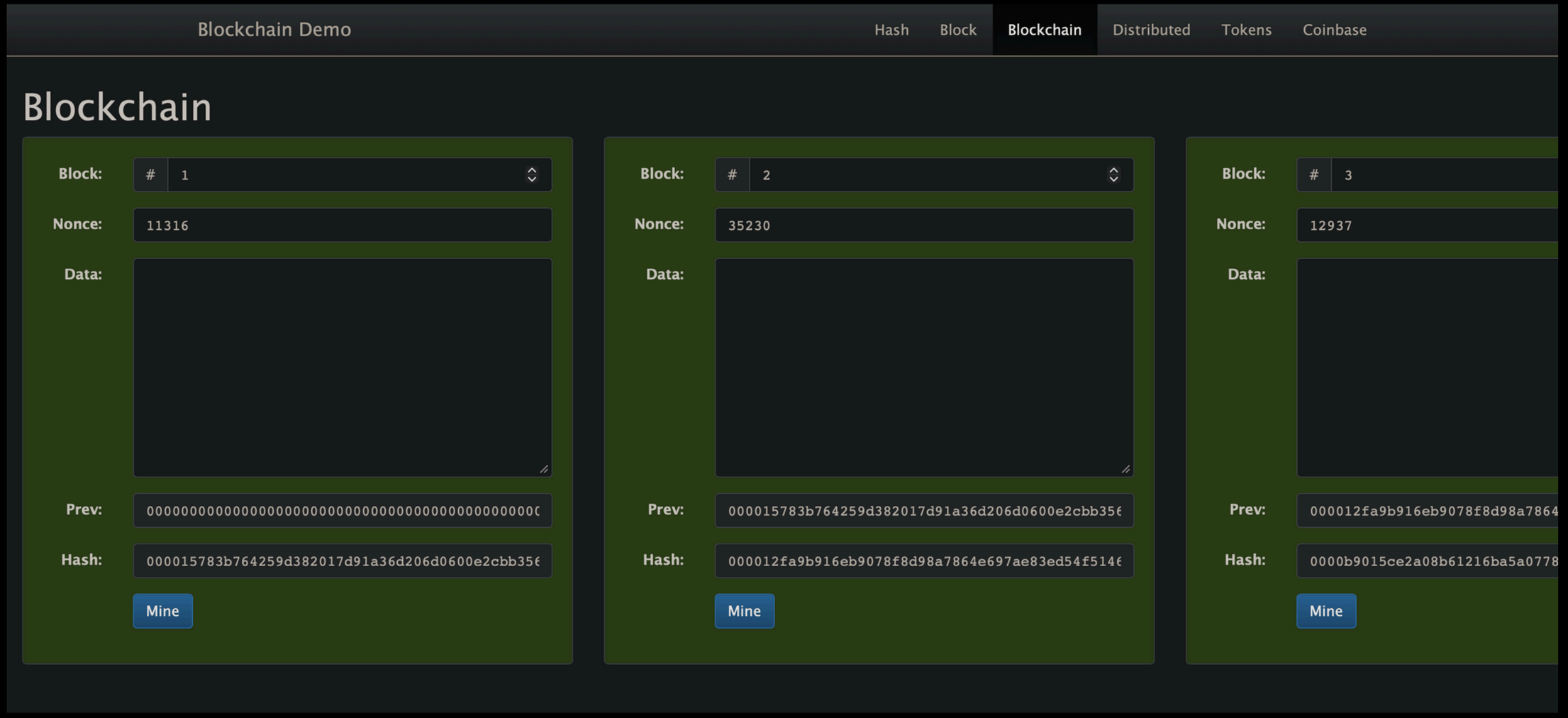
If data is tampered, hashes don’t match — chain breaks → tamper evident.

Crypto Connection:

Uses hashing (SHA256) + asymmetric encryption for signing and verification.

Lets try creating a chain hands on

https://andersbrownworth.com/blockchain/blockchain



Finally Digital Signatures & Certificates

Digital Signatures & Certificates

- How do we prove identity online?
  - A digital signature = encrypted hash of data.
  - Ensures integrity (no tampering) and authenticity (sender verified).
  - Certificates (via Certificate Authorities) bind a public key to an identity.
- Example:
  - PDF signatures, signed emails, and SSL certificates — all use digital signatures.

BLOG

Understanding Digital Signatures

Released: February 01, 2021

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, IDENTITY THEFT AND PERSONAL CYBER THREATS, CYBER THREATS AND ADVISORIES

What is a digital signature?

A digital signature—a type of electronic signature—is a mathematical algorithm routinely used to validate the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document). Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents. In emails, the email content itself becomes part of the digital signature. Digital signatures are significantly more secure than other forms of electronic signatures.

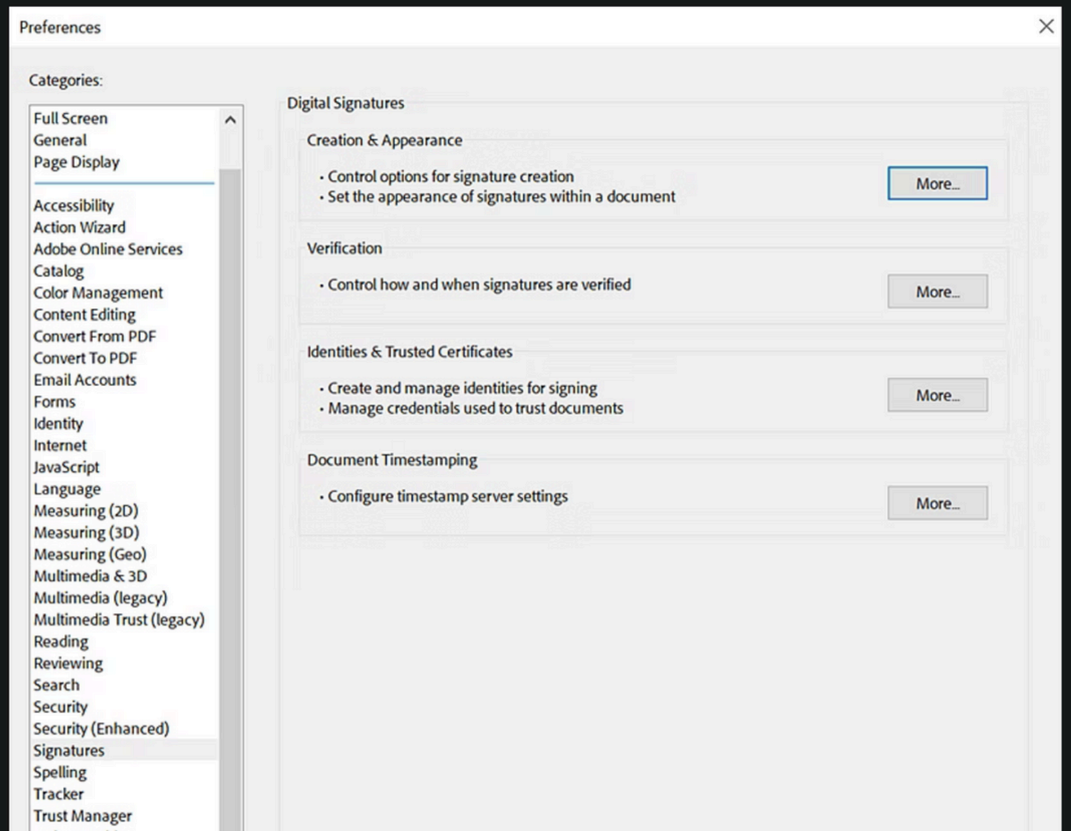
Validating digital signatures

Why validate a digital signature?

When you receive a signed document, you may want to validate its signature to verify the signer and the signed content. Depending on how you've configured your application, validation may occur automatically. Signature validity is determined by checking the authenticity of the signature's digital ID certificate status and document integrity.

To verify authenticity, the validator checks if the signer's certificate or its parent certificates are trusted. The validity of the signing certificate is also checked based on the user's Acrobat or Acrobat Reader settings.

To verify document integrity, the validator checks if the signed content was altered after signing. If changes were made, the verification ensures that the signer allowed the changes.



Class Summary – Hidden Truths in Plain Sight

What We Explored Today:

- **Steganography — the art of hiding information within images, text, and audio.**
- **Digital Watermarking — embedding authenticity, not secrets.**
- **Detection & Forensics — spotting hidden data through patterns, metadata, and anomalies.**
- **Everyday Crypto — E2EE, SSL/TLS, blockchain, and how modern trust is built on math.**
- **Cicada 3301 — when puzzles met cryptography and the internet became a playground for the curious.**

Key Takeaways:

- **“It’s not always about encrypting — sometimes it’s about hiding.”**
- **Secrets live in pixels, patterns, and protocols.**
- **The same techniques that protect truth can also conceal lies — it depends on who holds the key.**