![deeptruth logo]

"Soon, it's going to get to the point where there is no way that we can actually detect [deepfakes] anymore, so we have to look at other types of solutions." – Hao Li, Professor at University of Southern California

Advances in digital media altering technologies ("deepfakes" and "synthetic media") and their potential impacts are triggering widespread concern among politicians, media, businesses, consumers, and academics. The consequences of high-tech counterfeit media spreading disinformation are significant: fraud, manipulation, deception, conflict, and influence.

Businesses are increasing their reliance on digital media to substantiate workflow processes. The growing ease of altering digital content will compel industries to establish chain-of-custody solutions to protect authenticity of their digital assets.
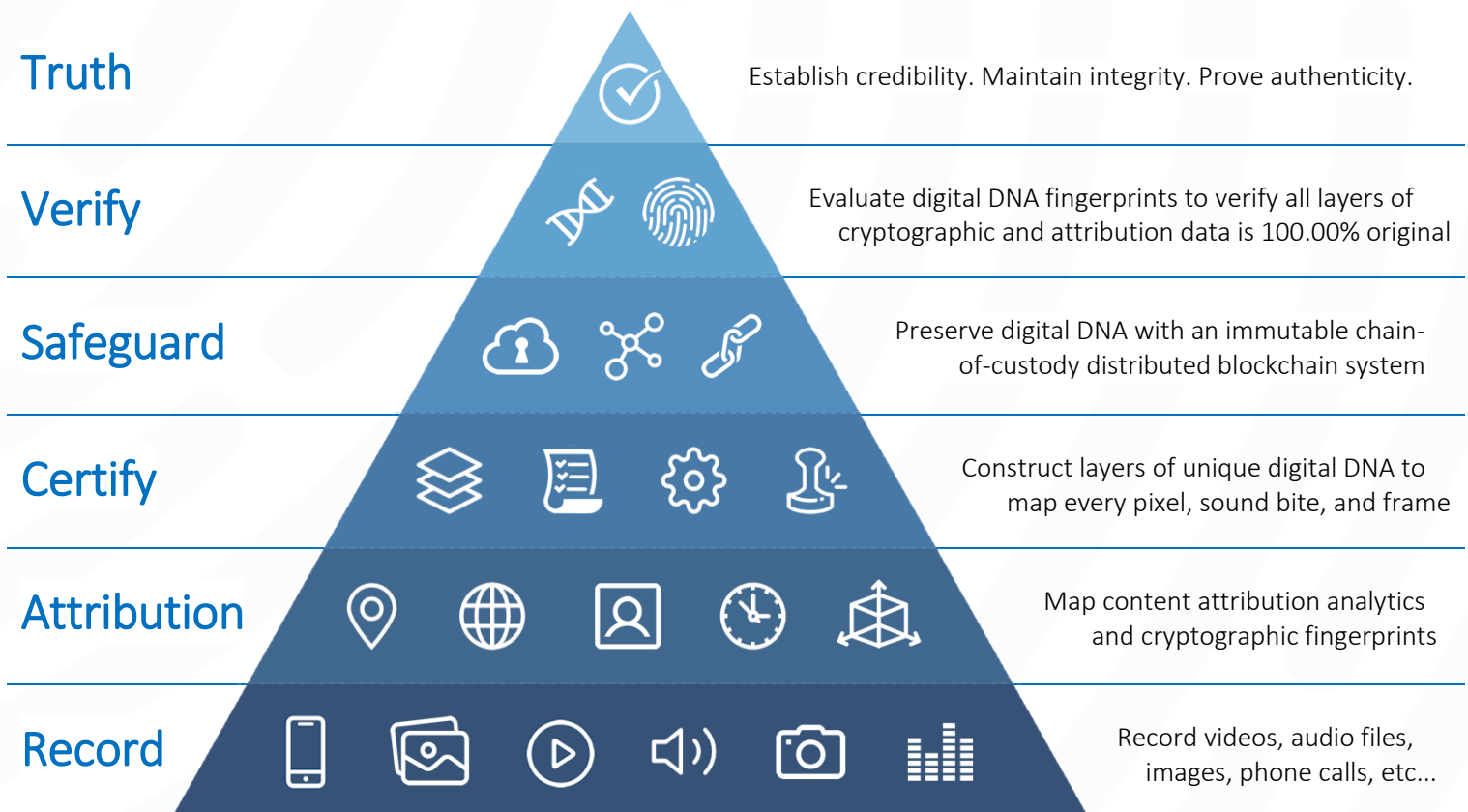
The challenges of synthetic media have entered the national conversation and the tech industry is facing mounting pressure to solve them. The predominant efforts by leading tech companies have focused on various forensic techniques to identify and discredit counterfeit content. Although defense is vital in the fight against deepfakes, it's a battle that can't be won. The volume, velocity, and sophistication of synthetic media will continue to accelerate and outpace all types of forensic efforts.

The only solution to win the long fight against synthetic media is to go on the offense and protect the credibility and integrity of digital assets from end-to-end. Every video, image, and audio must be recorded and protected in a manner that makes them impossible to modify or manipulate without detection.
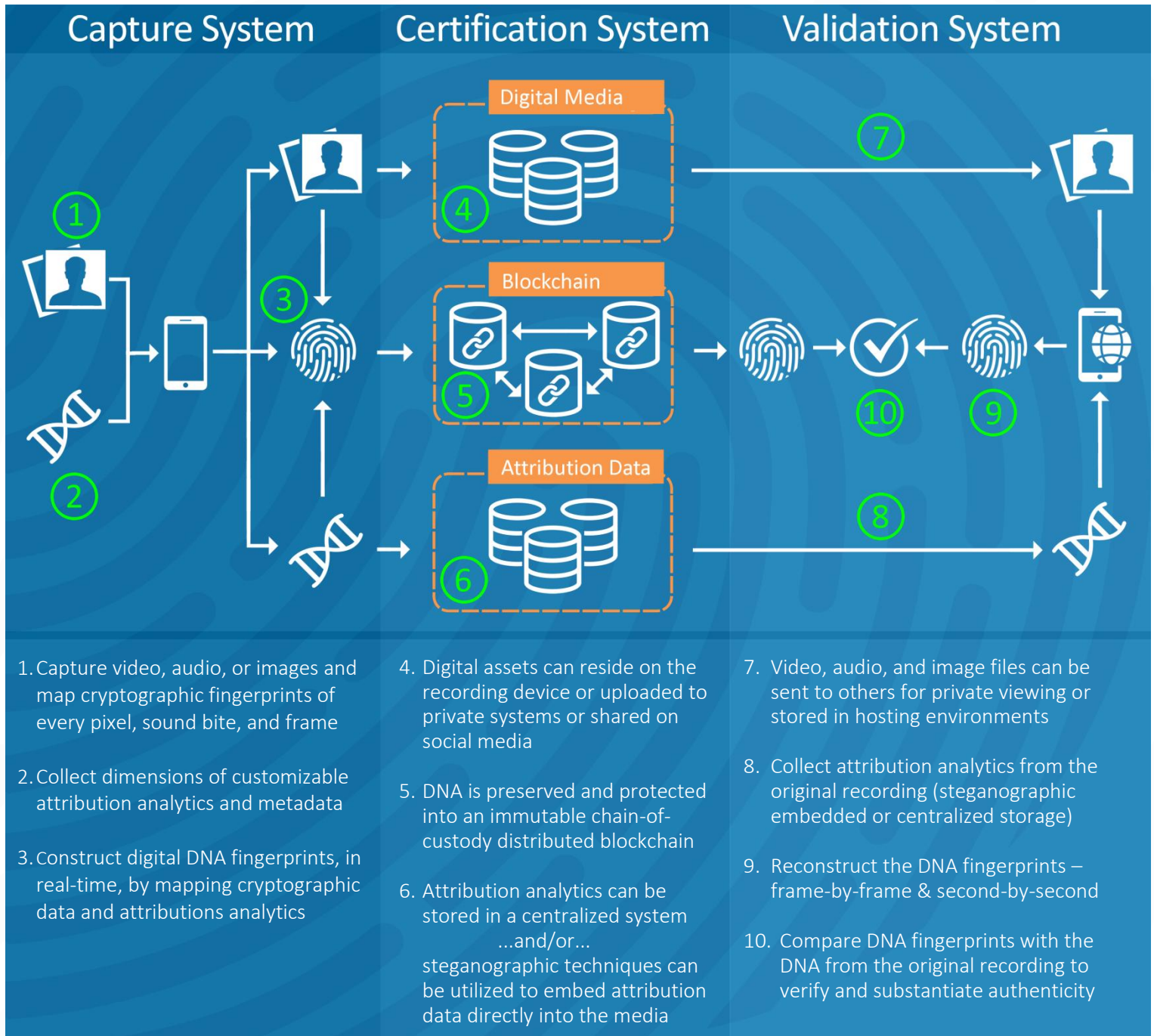
The internet needs a notary to protect digital media. DeepTruth is the solution.

DeepTruth's multi-patented framework records unbreakable media by constructing cryptographic DNA fingerprints–second-by-second. The DNA maps every pixel, sound bite, and frame, during recording, while simultaneously layering dimensions of content attribution analytics. The fingerprints are preserved, in real-time, to an immutable distributed blockchain ledger.

The integrity and authenticity of digital assets can be verified, at any time, by reconstructing the digital DNA fingerprints and comparing it to the original DNA. If any sub-second of a digital asset has a single pixel modified or sound bite altered or any of the dimensions of content attribution data changed, it will be flagged. Here is the hierarchy of DeepTruth's protection:

Truth	Establish credibility. Maintain integrity. Prove authenticity.
Verify	Evaluate digital DNA fingerprints to verify all layers of cryptographic and attribution data is 100.00% original
Safeguard	Preserve digital DNA with an immutable chain-of-custody distributed blockchain system
Certify	Construct layers of unique digital DNA to map every pixel, sound bite, and frame
Attribution	Map content attribution analytics and cryptographic fingerprints
Record	Record videos, audio files, images, phone calls, etc...

www.deeptruth.com

DeepTruth provides the framework to build flexible and scalable solutions. Our innovations are disruptive and our intellectual property has the capacity to transform markets/industries and dramatically shift competitive advantages. Here's our system:

Capture System
Certification System
Validation System

1. Capture video, audio, or images and map cryptographic fingerprints of every pixel, sound bite, and frame

2. Collect dimensions of customizable attribution analytics and metadata

3. Construct digital DNA fingerprints, in real-time, by mapping cryptographic data and attributions analytics

4. Digital assets can reside on the recording device or uploaded to private systems or shared on social media

5. DNA is preserved and protected into an immutable chain-of-custody distributed blockchain

6. Attribution analytics can be stored in a centralized system
...and/or...
steganographic techniques can be utilized to embed attribution data directly into the media

7. Video, audio, and image files can be sent to others for private viewing or stored in hosting environments

8. Collect attribution analytics from the original recording (steganographic embedded or centralized storage)

9. Reconstruct the DNA fingerprints – frame-by-frame & second-by-second

10. Compare DNA fingerprints with the DNA from the original recording to verify and substantiate authenticity

If you are interested in learning more about our IP portfolio, please visit us at: www.deeptruth.com/demo.

U.S. Patent #10,348,505 – Systems and techniques for validation of trusted media data
U.S. Patent #10,355,865 – Systems and techniques for certification of trusted media data
U.S. Patent #10,560,261 – Systems and techniques for capture of trusted media data
U.S. Patent #10,853,456 – Authenticating media data based on steganographic and blockchain techniques