Fraunhofer FOKUS
Institut für Offene Kommunikationssysteme

© Philipp Plum/ Fraunhofer FOKUS

Content Provenance & Authenticity

Securing value through digital infrastructures

Andy Neparidze

Fraunhofer FOKUS

Schedule

No	Week	Date	Topic
1	42	16.10.2023	Introduction and Framework
2	43	23.10.2023	Web Technologies Basics & Media Entertainment for the Web
3	44	30.10.2023	Foundations of Media Streaming
4	45	06.11.2023	Advanced Media Streaming
5	46	13.11.2023	Multiscreen Technologies and Standards
6	47	20.11.2023	Context-Aware Media Streaming & Encoding
7	48	27.11.2023	Dynamic Advertisement
8	49	04.12.2023	Media Players - dash.js, Exoplayer
9	50	11.12.2023	HbbTV and Smart TV
	51	18.12.2023	Holiday break
	52	25.12.2023	Holiday break
	1	01.01.2024	Holiday break
10	2	08.01.2024	Media Delivery in 5G Networks (1)
11	3	15.01.2024	Media Delivery in 5G Networks (2)
12	4	22.01.2024	Interoperable Web-supported Learning Technologies
13	5	29.01.2024	Metaverse Platforms and Technologies
14	6	05.02.2024	Securing Content-Provenance and Authenticity
15	7	12.02.2024	Exercise and Test Preparation - ONLINE VIA ZOOM - VERY IMPORTANT TO JOIN!!!
16	8	19.02.2024	Written Test first slot (60+10min) - ONLINE (follow instructions/announcements in ISIS)

Agenda

- Motivation
- Distributed Knowledge
  - Blockchain Technologies
  - Distributed File Storage
- Application Areas
  - Securing Value of Digital Art
  - Verification of Authenticity of Physical Products

Motivation

Fraunhofer FOKUS

Source: https://www.youtube.com/watch?v=cQ54GDm1eL0

Fraunhofer FOKUS

Motivation

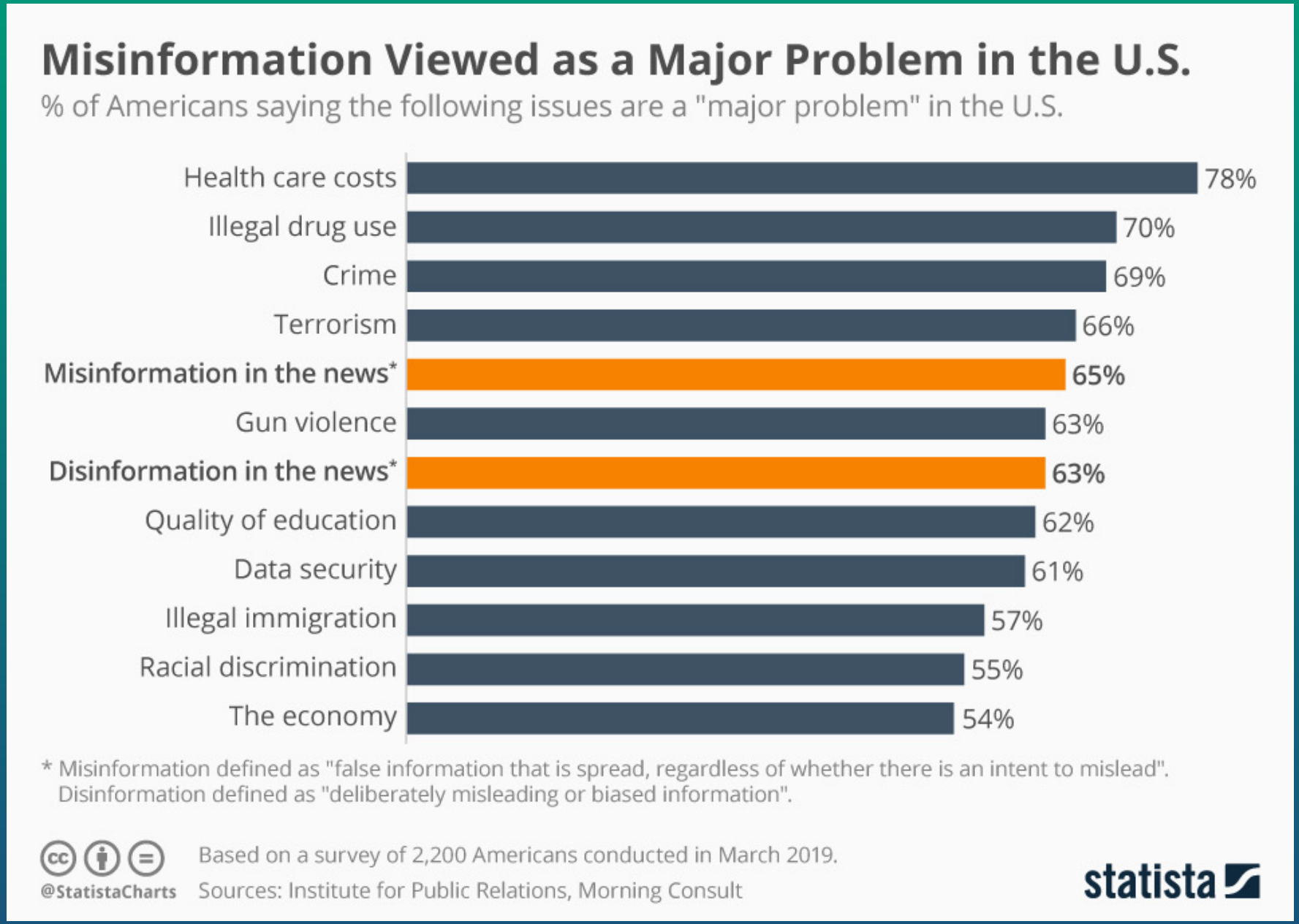
- Deepfakes
  - ✓ Videos generated by Deep Neural Networks
  - ✓ It only takes 1 picture of target person

- Fake News
  - ✓ Jokes that are believed to be true
  - ✓ Scams to make money
  - ✓ Political disinformation
  - ✓ Conspiracy Theories
  - ✓ Insiders – fake / non existing characters

- Pirate Copies
  - ✓ Duplicates of illegally acquired media

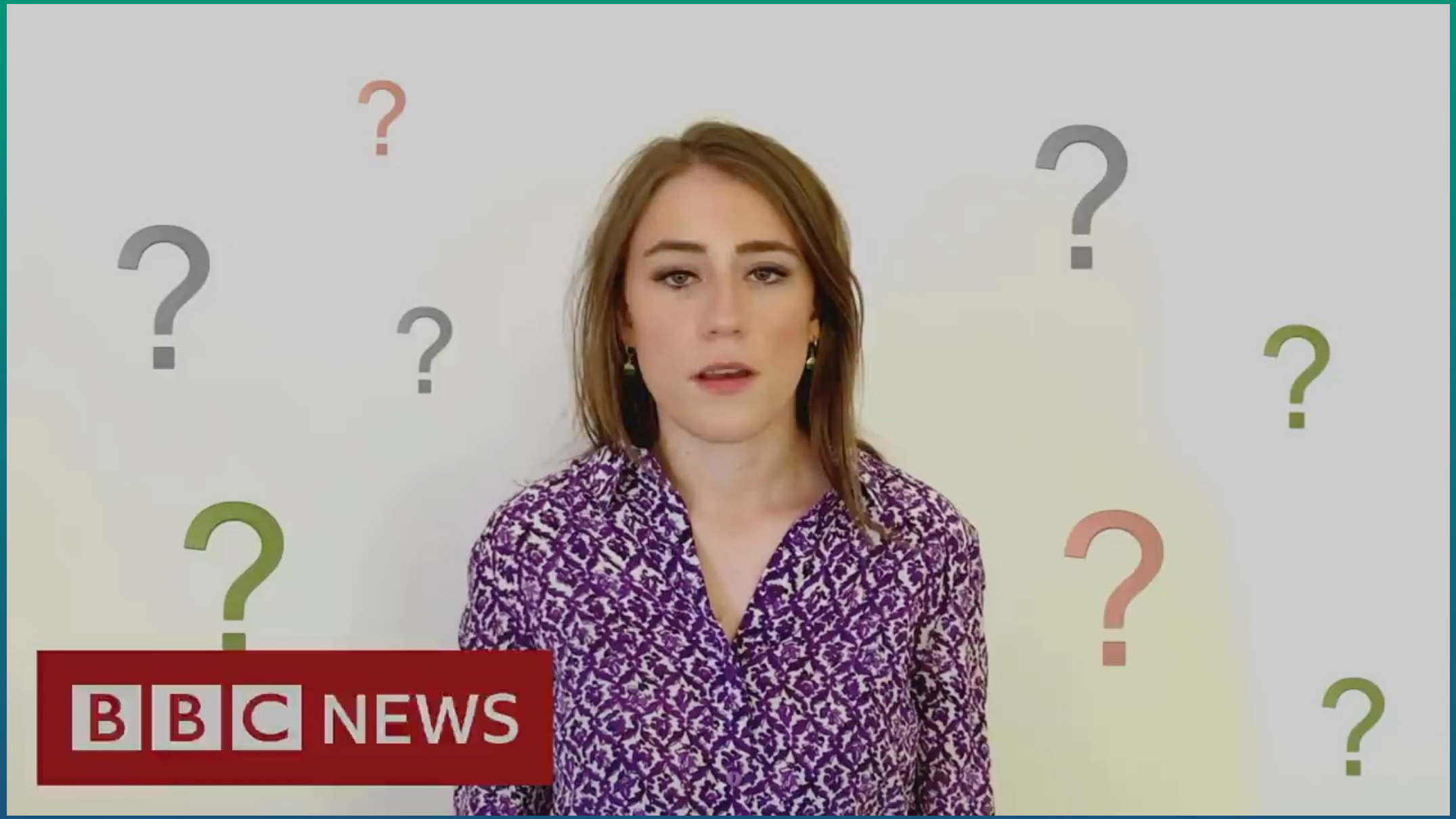
Fraunhofer FOKUS

Source: https://www.youtube.com/watch?v=F4G6GNFz0O8



Source: https://cdn.statcdn.com/Infographic/images/normal/18538.jpeg

Fraunhofer FOKUS



Source: BBC https://www.youtube.com/watch?v=UAy6PI5UtSU

Coalition for Content Provenance and Authenticity

C2PA – Need & Partners

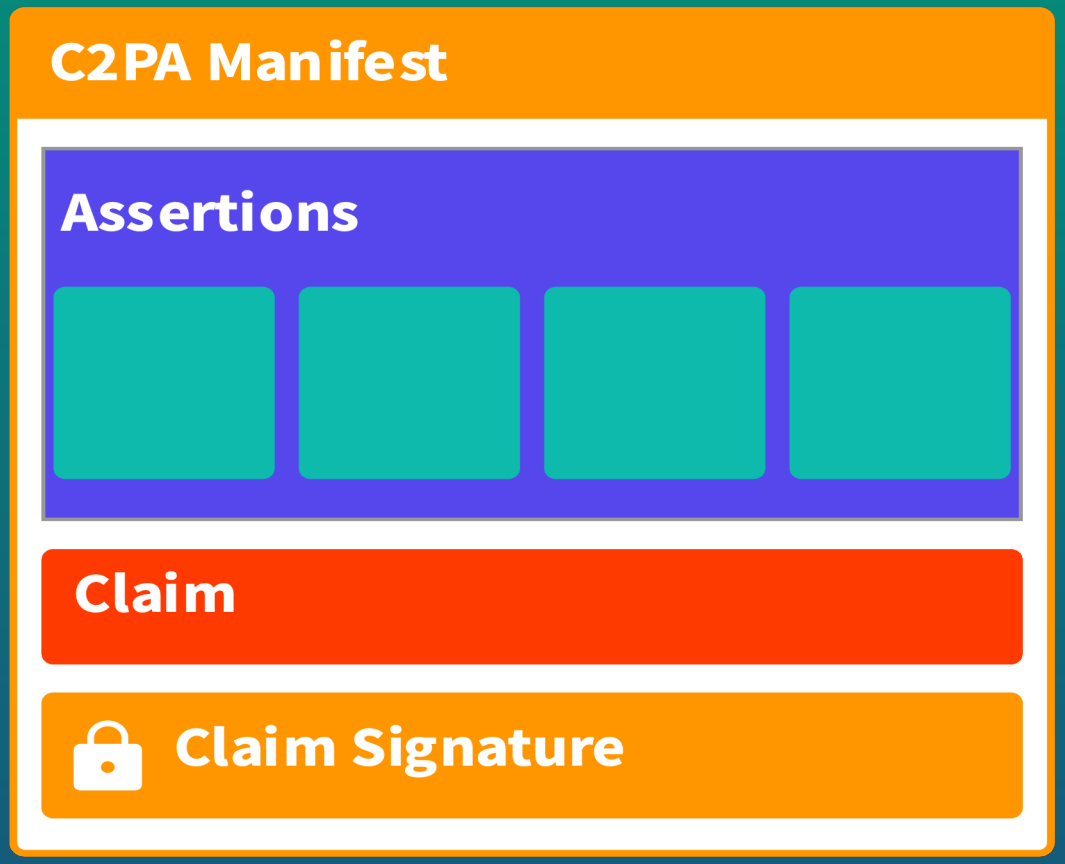
- Partners:
  - Microsoft
  - BBC
  - Adobe
  - intel
  -
  - And many others

- Need
  - Combat Deep Fakes
  - Copyright
  - Combat Disinformation/Missinformation

Source: https://c2pa.org/membership/

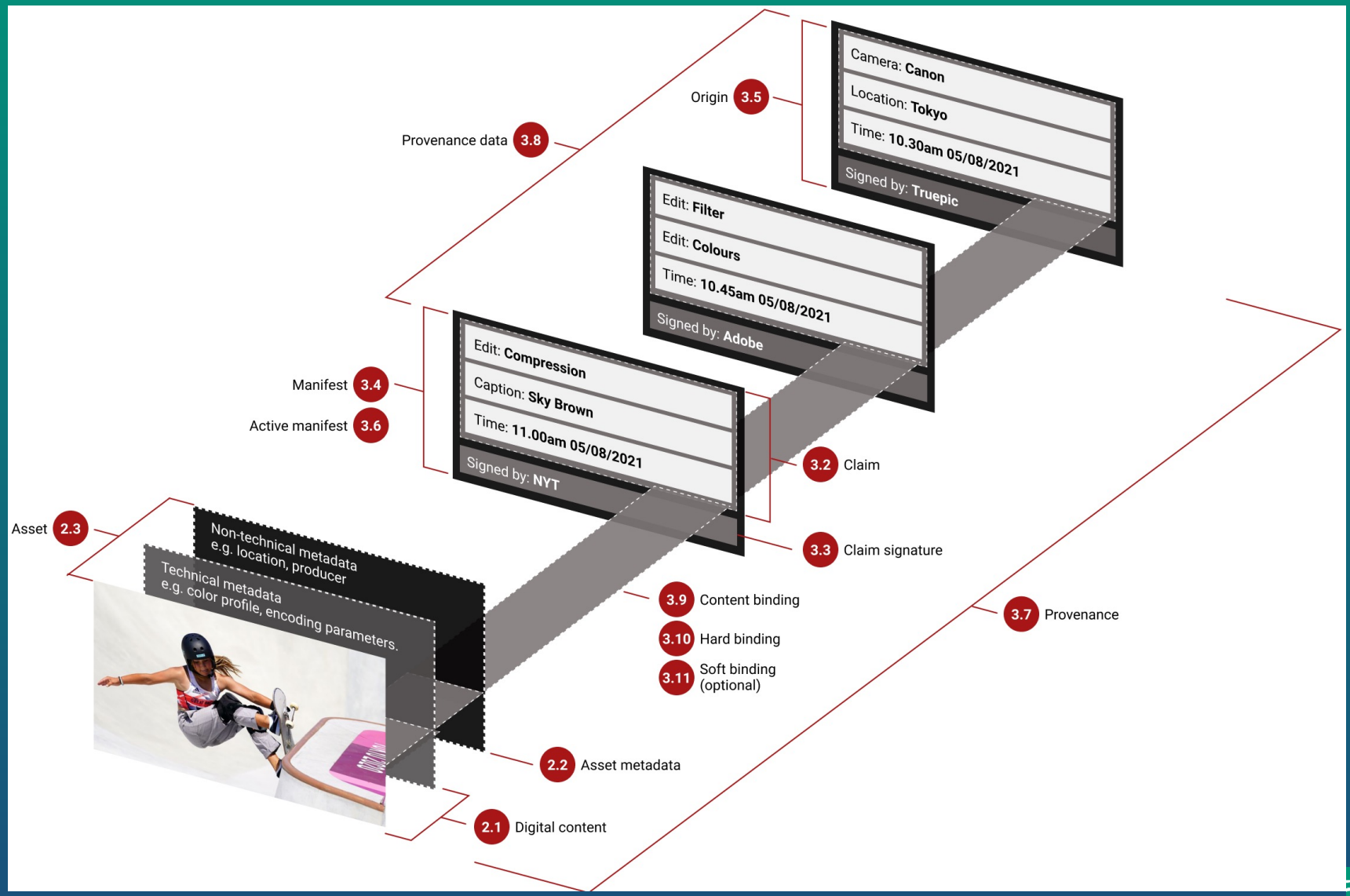
C2PA – Functionality

- Embedding signed manifest file into a media file
  - ✓Generate manifest describing content
  - ✓Sign manifest with publisher's signature
  - ✓Embed manifest into media
- Being able to extract embedded data and verify origin
  - ✓For example: a browser extension reads data
  - ✓Communicate result to the user
- Being able to perform content based search
  - ✓There is a database for lookup
  - ✓Needed when manifest gets removed



Fraunhofer FOKUS

C2PA – Chain of Provenance



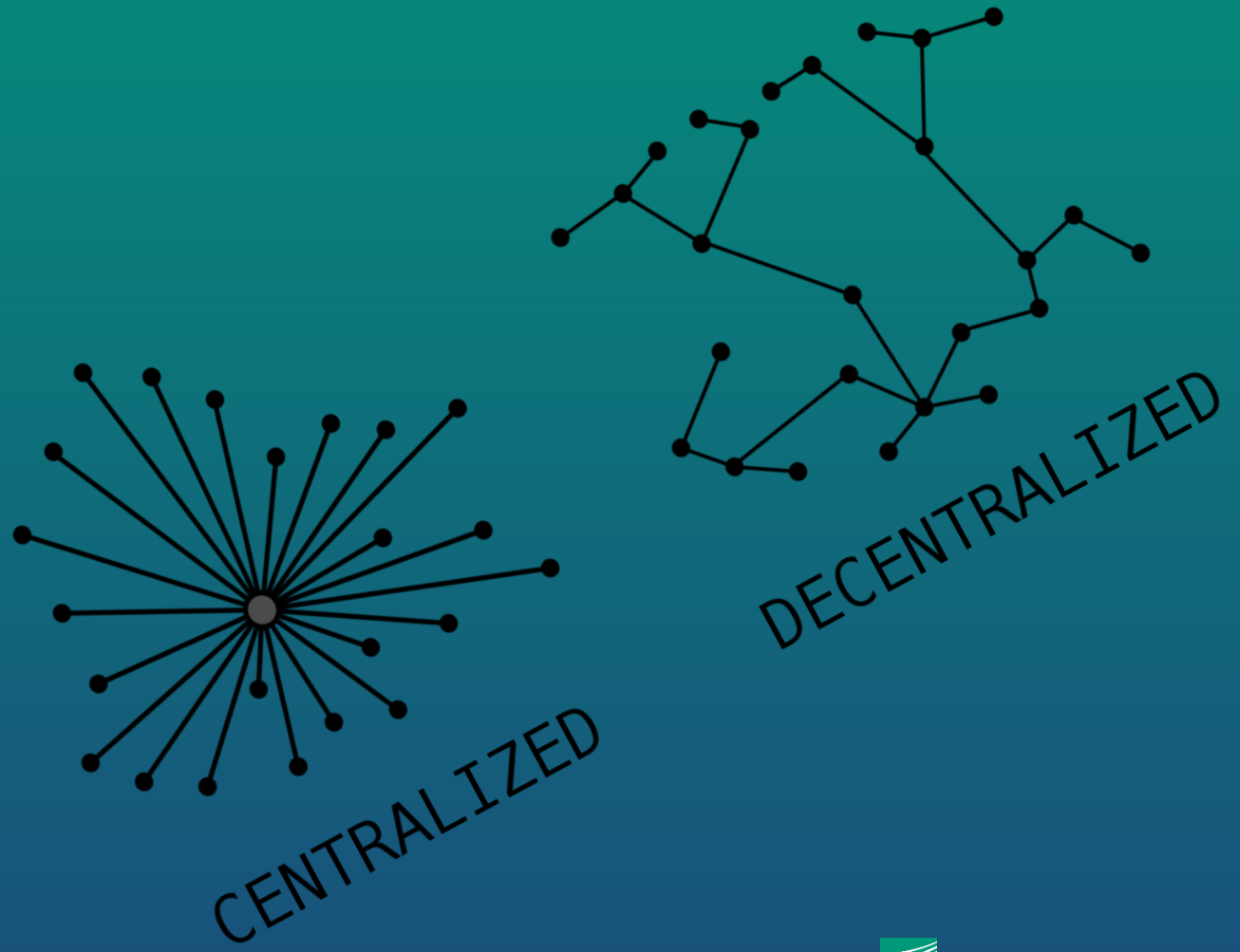
Source: https://c2pa.org/public-draft/

Fraunhofer FOKUS

Need of Distributed Knowledge → DLT (Blockchain) & IPFS

- **Pros of a Centralized System**
  - ✓ Easier deployment
  - ✓ Can be built faster
  - ✓ Easier to maintain
  - ✓ Useful when data is centrally controlled

- Pros of a Distributed System
  - ✓ Fault-tolerant
  - ✓ Transparent and secure
  - ✓ Promotes resource sharing
  - ✓ Extremely scalable



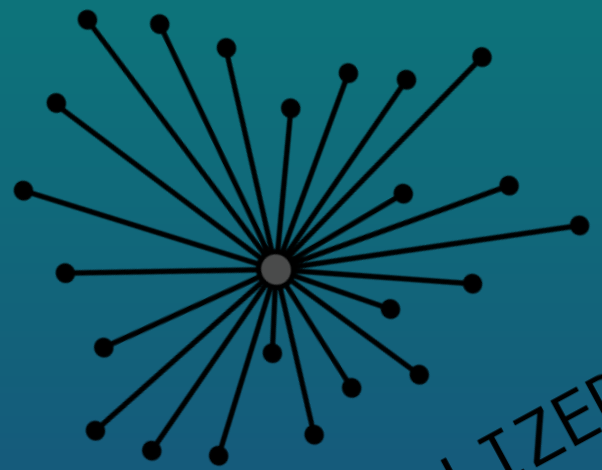
Source: https://berty.tech/blog/decentralized-distributed-centralized, https://en.wikipedia.org/wiki/Decentralised_system

Fraunhofer FOKUS

Need of Distributed Knowledge → DLT (Blockchain) & IPFS

- **Cons of a Centralized System**
  - ✓ Trust Lies on Central Institution
  - ✓ Higher security and privacy risks for users
  - ✓ Prone to failures
  - ✓ If a user is far from the server delays to receive data
  - ✓ Limited availability of files, what is lost is lost forever

- Cons of a Distributed System
  - ✓ More difficult to deploy
  - ✓ Maintanance costs are considerably higher



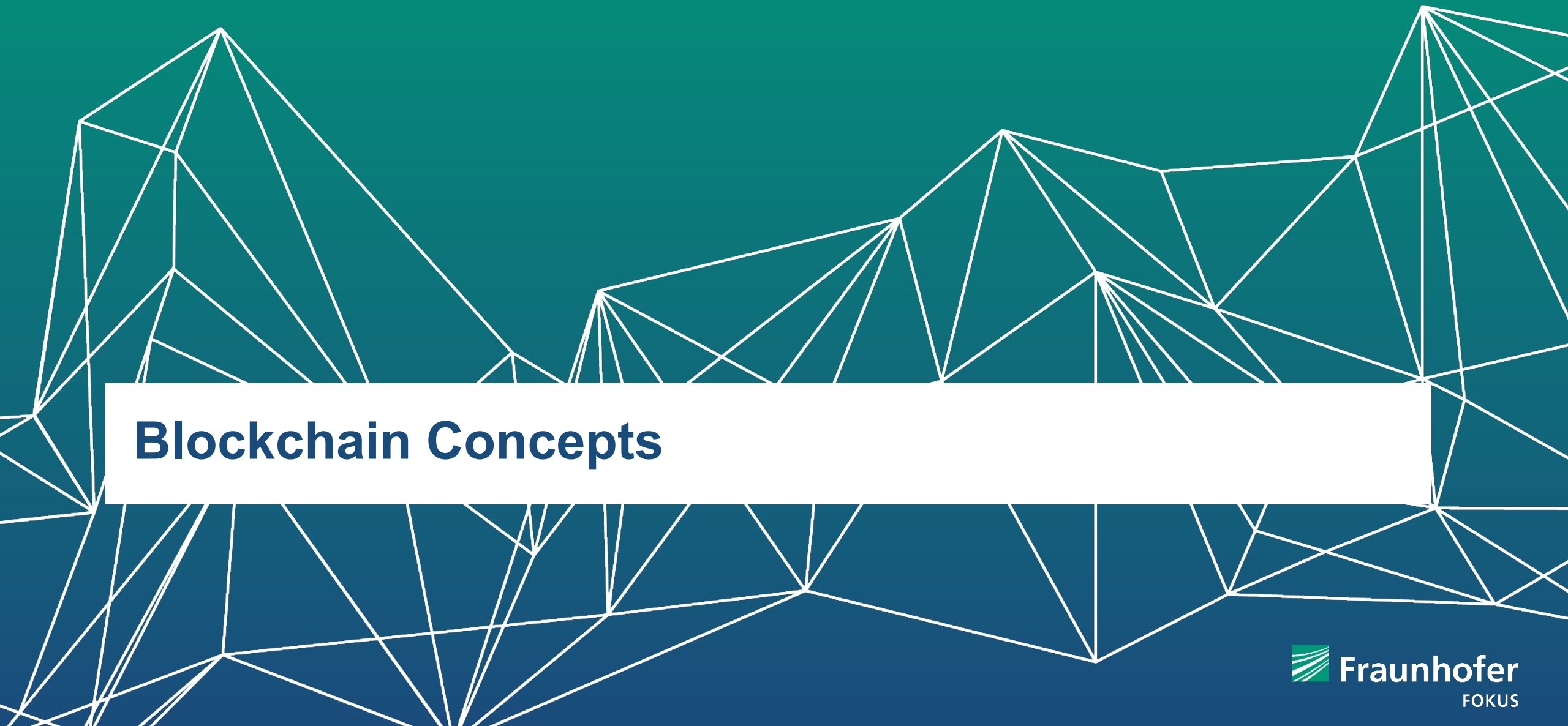
CENTRALIZED

DECENTRALIZED

Source: https://berty.tech/blog/decentralized-distributed-centralized, https://en.wikipedia.org/wiki/Decentralised_system

Fraunhofer FOKUS

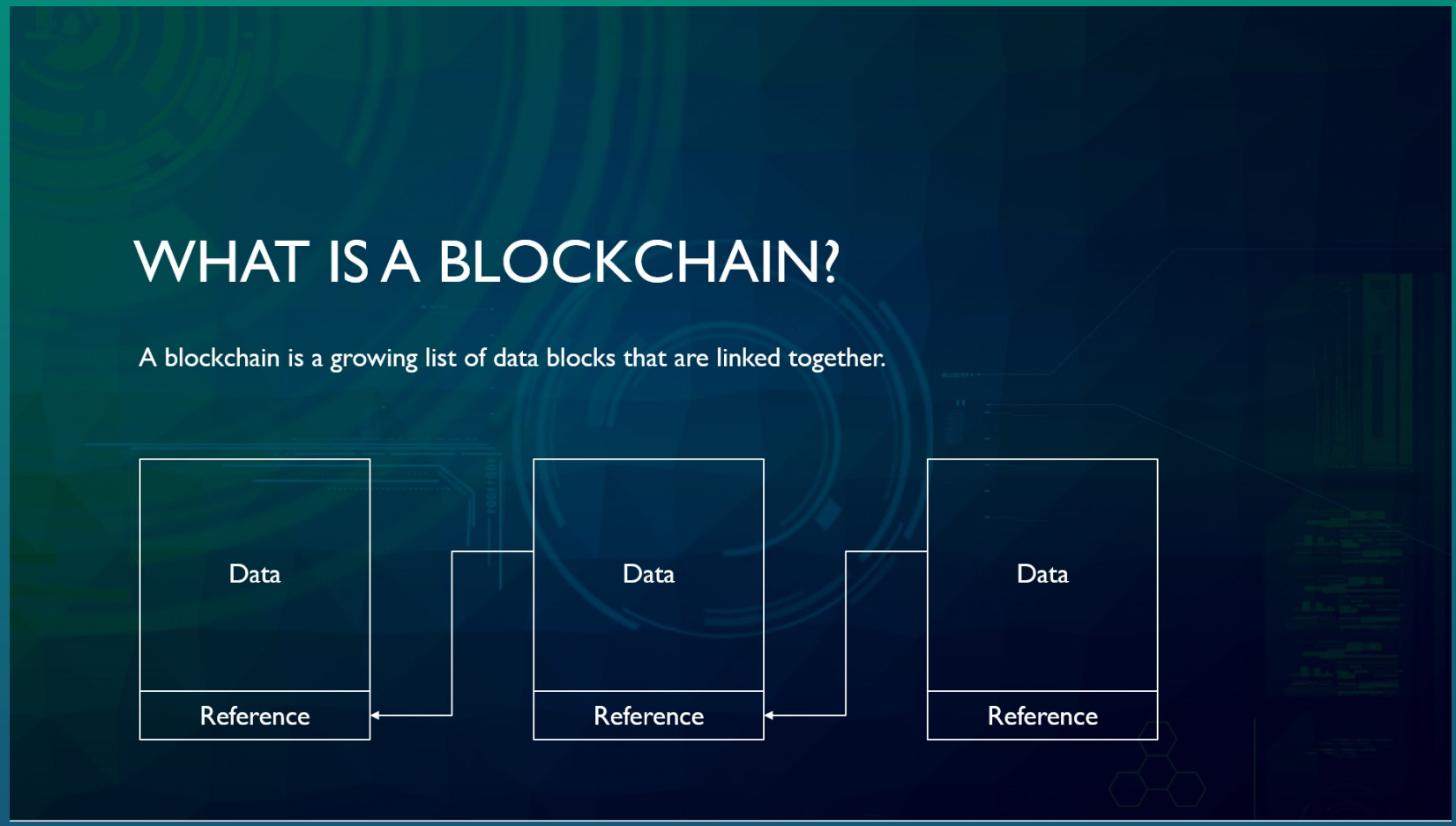
Blockchain Concepts



Fraunhofer FOKUS

Blockchain - Basic Principles

- Distributed Knowledge
- Peer-to-Peer Transmission
- Transparency
- Immutable Records



Source: https://originstamp.com/blog/blockchain-technology-ppt-presentation/

Fraunhofer FOKUS

Blockchain from The Business Perspective

- Transaction costs
  - ✓ Transaction fee is charged when performing transactions
- Risks
  - ✓ Too many transactions result in high costs
  - ✓ This requires thorough planning of how to use a blockchain system wisely
  - ✓ The transaction size is very important and could be bigger than the block size
- Benefits
  - ✓ Reading from the blockchain does not produce any fees
  - ✓ Trust in the system
  - ✓ Data is protected according to the principles of blockchain
- Cryptocurrencies
  - ✓ There is an abundance of Cryptocurrencies
  - ✓ Their value changes frequently

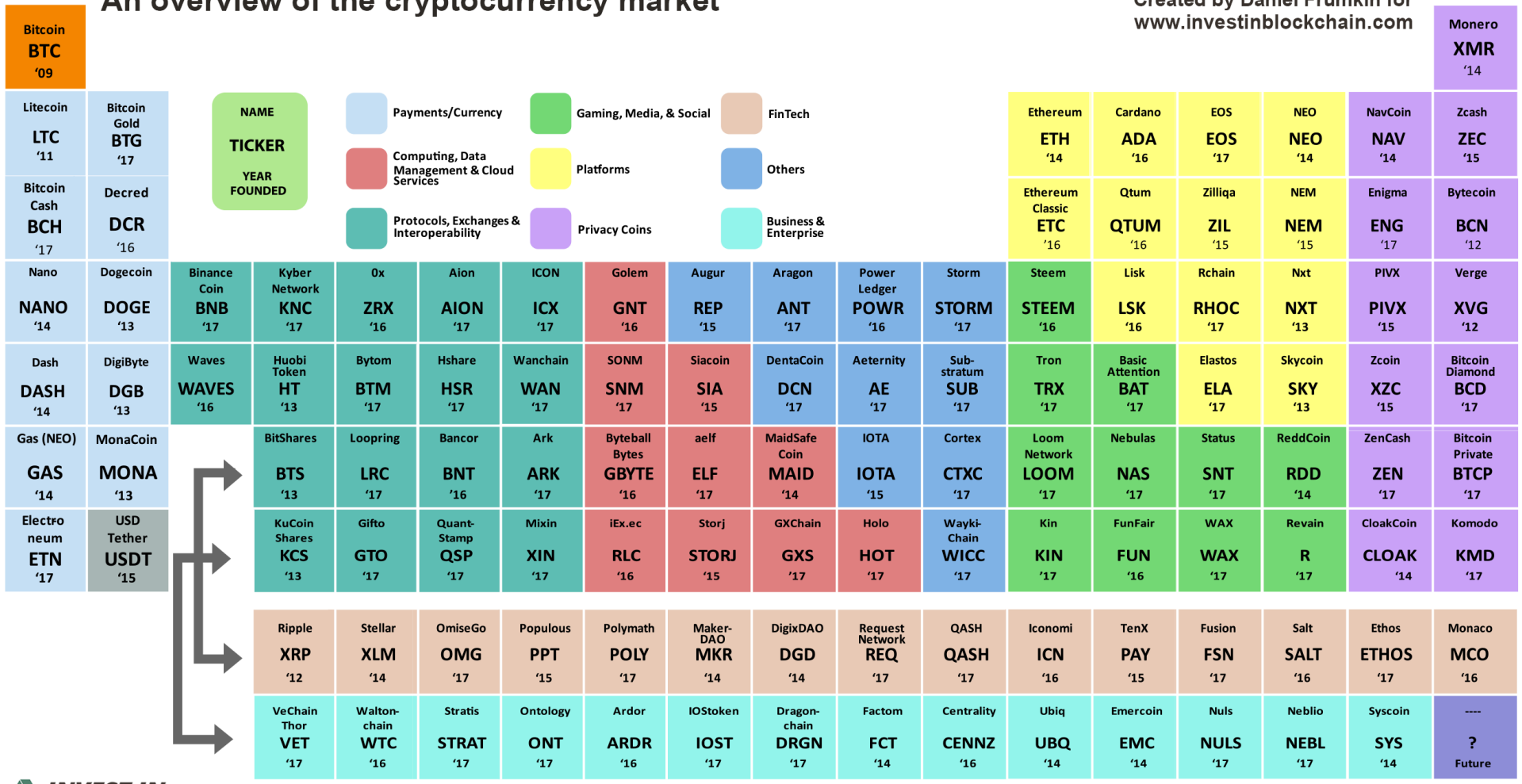
Source: https://de.wikipedia.org/wiki/Datei:Bitcoin_logo.svg, https://de.wikipedia.org/wiki/Ethereum

Fraunhofer FOKUS

The Periodic Table of Cryptocurrencies

An overview of the cryptocurrency market

Created by Daniel Frumkin for www.investinblockchain.com



INVEST IN BLOCKCHAIN

Source: https://www.investinblockchain.com/periodic-table-cryptocurrencies/

Fraunhofer FOKUS

Technical Aspects of Blockchain

- Example of a Technology Stack
  - ✓ Ethereum Based Blockchains(Ganache, Rinkeby Test Network) – Blockchain itself
  - ✓ Wallet(Metamask) – handles private keys and addresses
  - ✓ Framework For Writing and Migrating Smart Contracts(Truffle)
  - ✓ Language for Smart Contracts(Solidity)

- Getting Started
  - ✓ Setup a local Blockchain(Ganache) or use a test network(Rinkeby)
  - ✓ Setup a Truffle Instance
  - ✓ Setup a basic Smart Contract(at least one transaciton)
  - ✓ Compile Smart Contract and migrate to the Blockchain
  - ✓ Copy the addres and description(ABI) of Smart Contract and using Web3 libbrary call the transaction
  - ✓ Sign the transaction with Metamask(Or use your own private key to sigh with Web3)

Source: https://metamask.io/, https://trufflesuite.com/ganache/

Proof of Work VS Proof of Stake

Mining capacity depends on computational power

Validating capacity depends on the stake in the network

Miners receive block rewards to solve a cryptographic puzzle

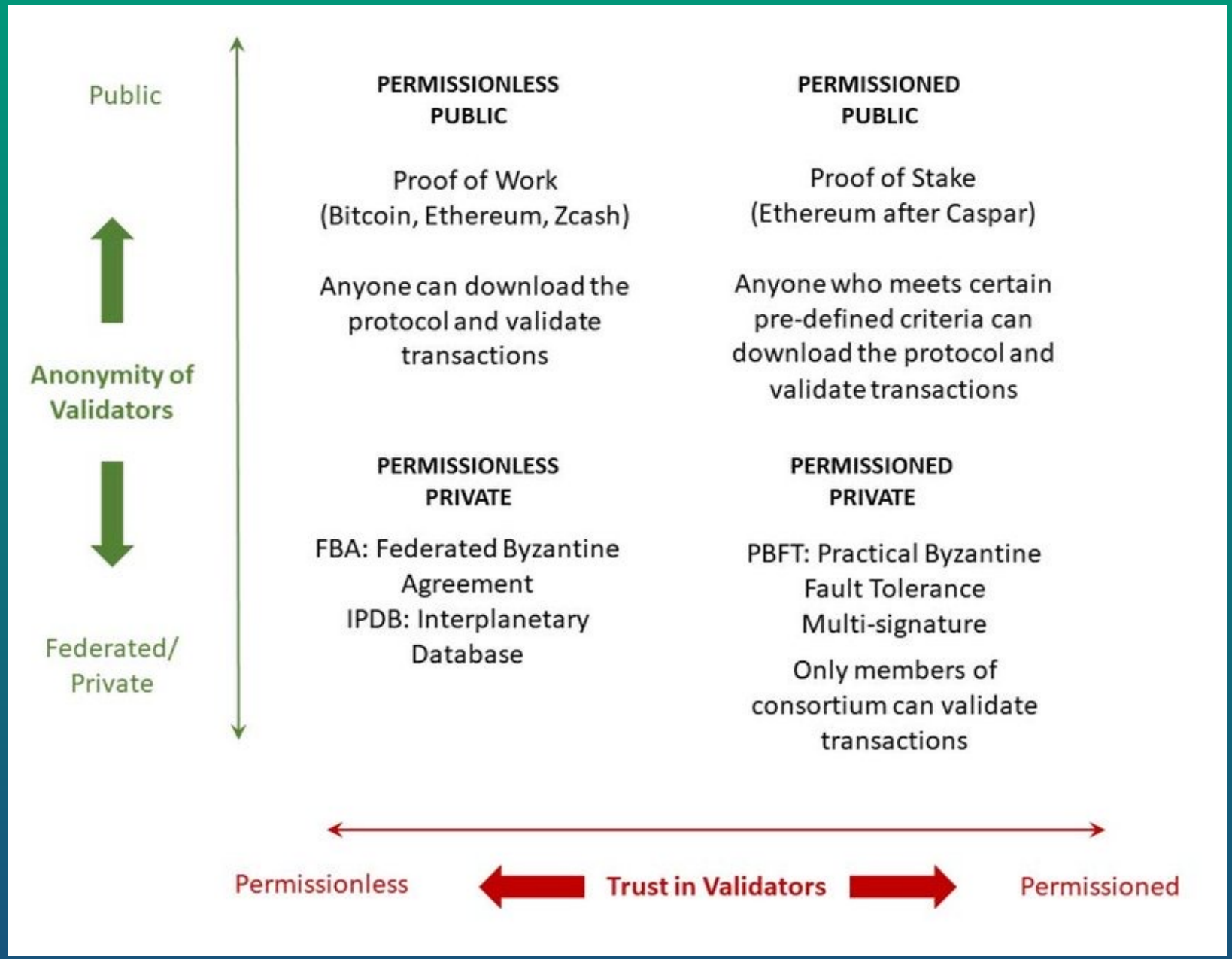
Validators do not receive a block reward, instead, they collect transaction fees as reward

Hackers would need to have a computer powerful than 51% of the network to add a malicious block, leading to 51% attack

Hacker would need to own 51% of all the cryptocurrency on the network, which is practically impossible and therefore, making 51% attacks impossible.

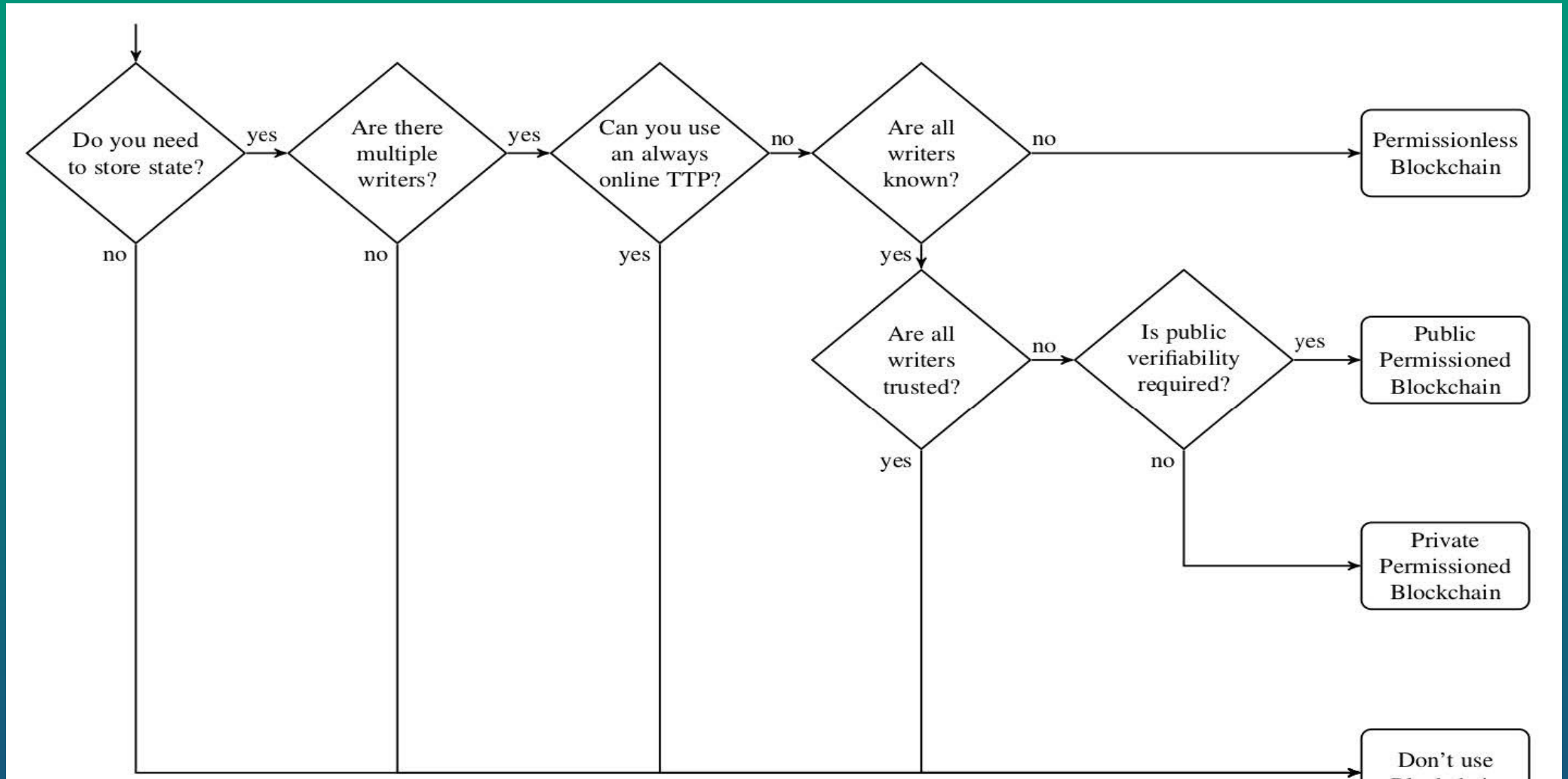
Source: https://sp-ao.shortpixel.ai/client/to_auto,q_glossy,ret_img,w_904,h_618/https://tradewithus.ch/wp-content/uploads/2021/04/proof_of_stake.jpg

Fraunhofer FOKUS



Source: https://www.researchgate.net/figure/Permissioned-versus-permissionless-blockchains-across-trust-and-anonymity-axes-This_fig2_329295642

Fraunhofer FOKUS



*TTP - trusted thitd party

Source: K. Wust and A. Gervais, "Do you need a blockchain?" IACR Cryptology ePrint Archive, vol. 2017, p. 375, 2017.

Fraunhofer FOKUS

Limited vs Unlimited Supply

- Liimited
  - ✓ The Bitcoin supply is limited to **21 million**
  - ✓ No Inflation
  - ✓ Deflation is the opposite of inflation
  - ✓ The money/asset in circulation gains value over time

- Unlimited
  - ✓ Etherium has constant flow of new assets added to the ecosystem
  - ✓ Inflation Possible
  - ✓ Having their own rules for issuing the new coins
  - ✓ Issuing a fixed amount of Ether per year

FT VS NFT

VS

- A 500€ bill in Berlin has the same value as the one in Munich – Fungible Token
- A unique paintings cannot be replaced with something else – Non Fungible Token

Source:https://upload.wikimedia.org/wikipedia/commons/7/77/Nota_500_euros.jpg

https://www.specialarabia.com/uploads/articles_uploads/img-2019_08_03_14_21_13-9600.jpg

Fraunhofer FOKUS

Divisibility vs Indivisibility

- Divisible
  - ✓ Can be divided in smaller parts
  - ✓ Can be distributed in smaller parts
  - ✓ For example: You could transfer 0.01 Euros or split 1 Euro into 50 Cents

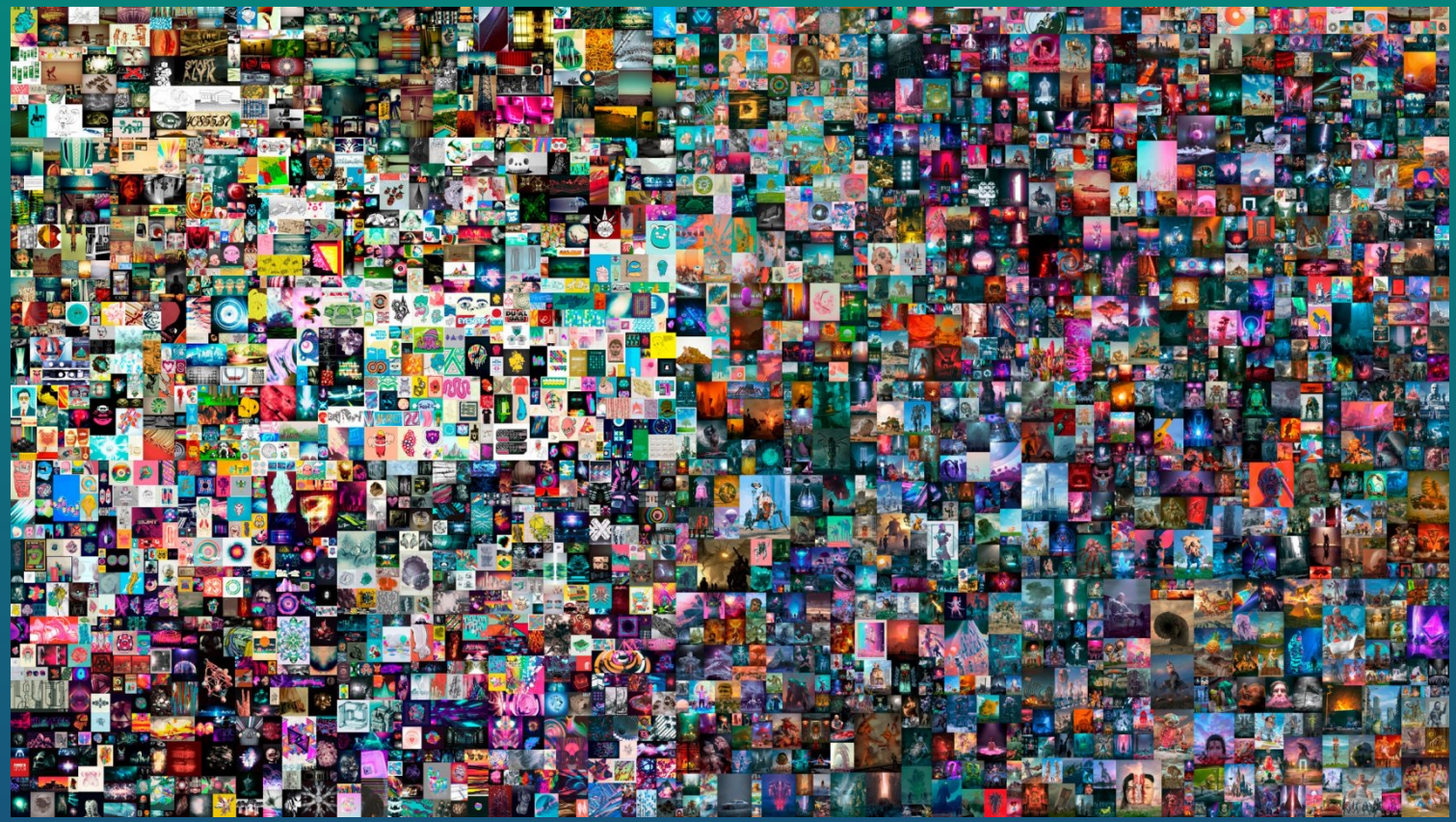
- Indivisible
  - ✓ Can NOT e divided in smaller parts
  - ✓ Distributed as a whole
  - ✓ If you sell your painting you sell it as a whole

Source: https://commons.wikimedia.org/wiki/File:10-Euro.svg, https://freesvg.org/

Fraunhofer FOKUS

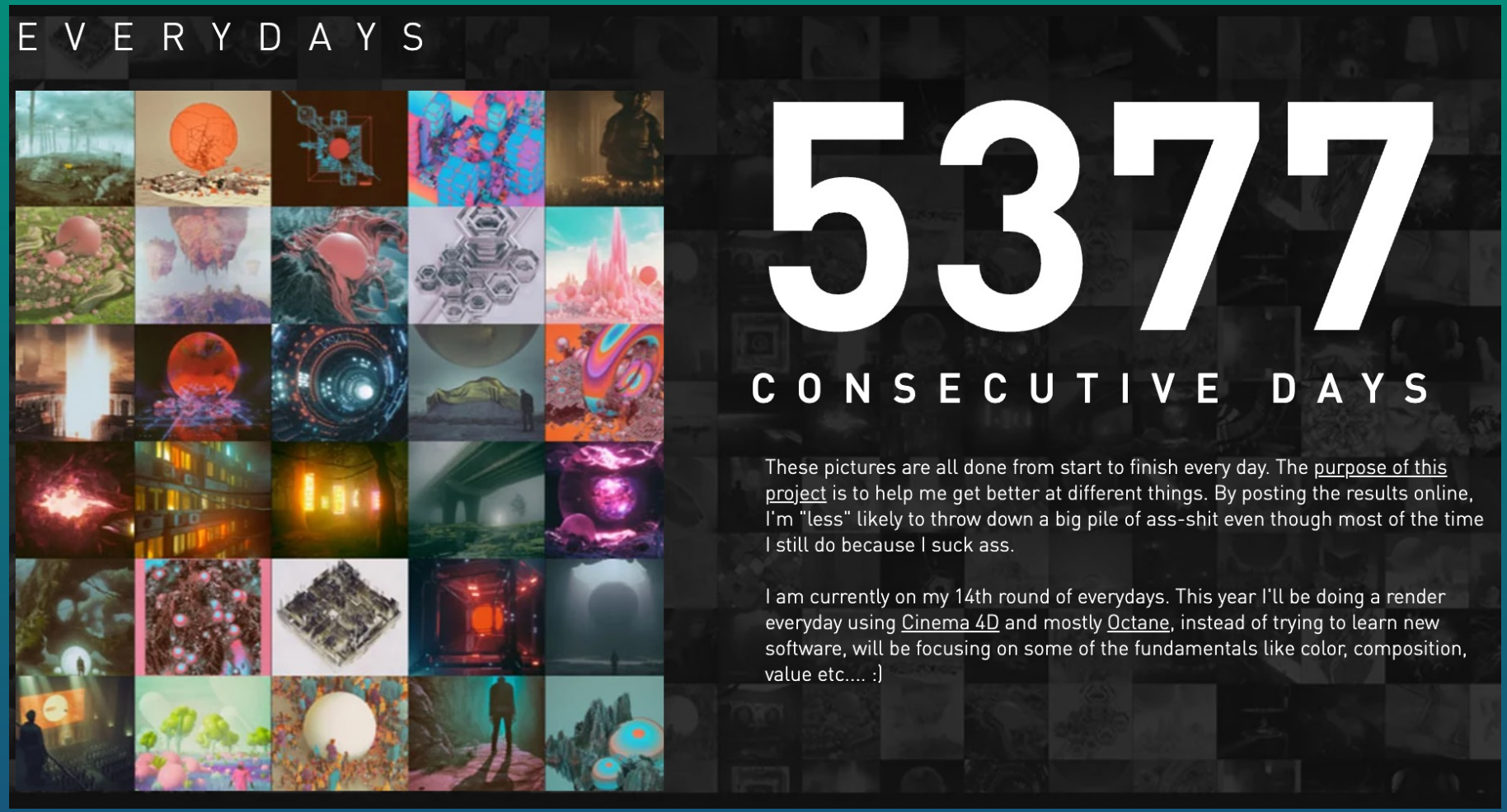
NFTs - Basic Principles

- An NFT is a Non-Fungible Token
- It **attributes ownership of a digital property to one single person**



Source: https://www.dezeen.com/2021/03/12/beeple-everydays-nft-christies-auction/

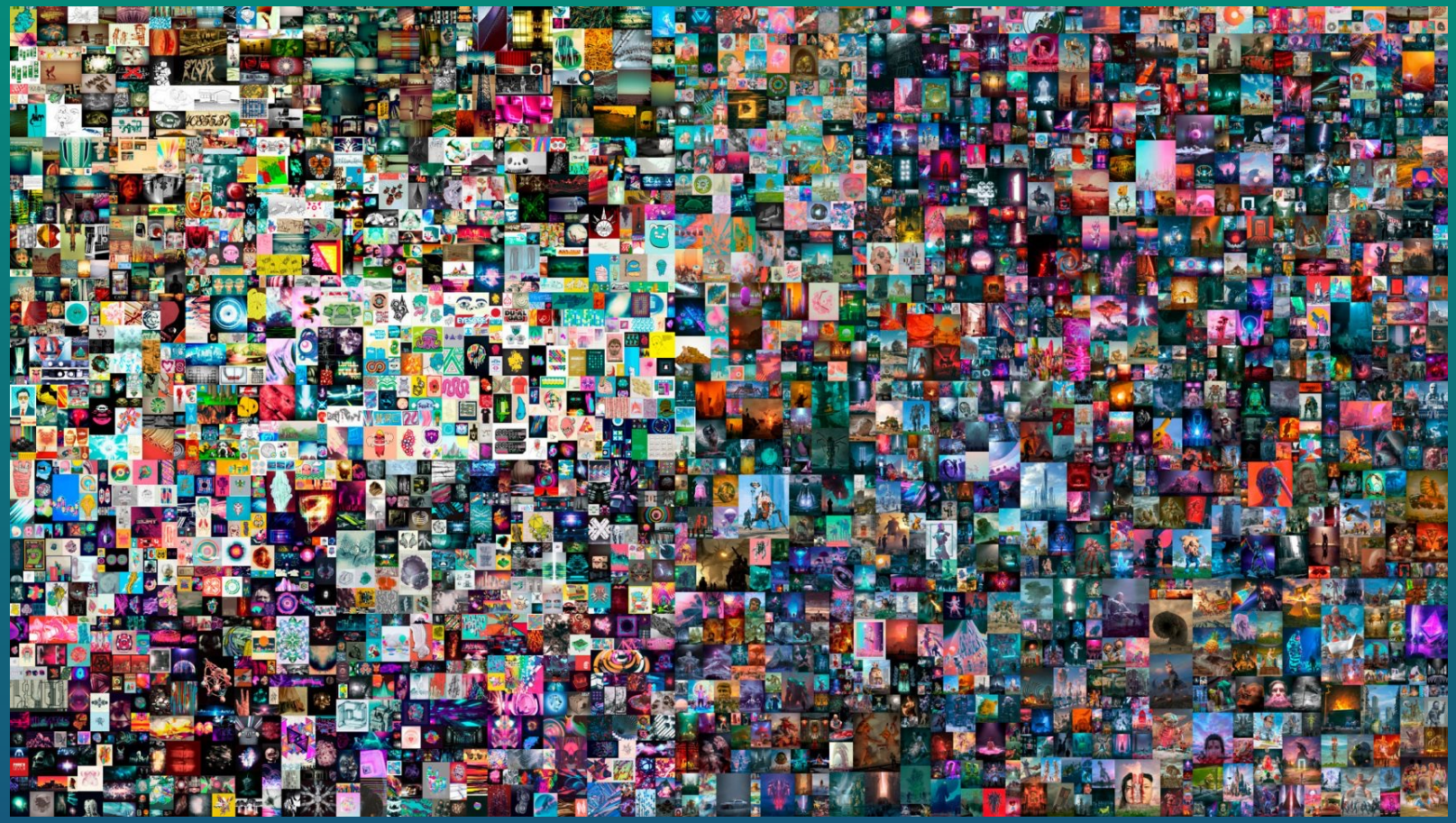
The Most Expensive NFT



Source: https://www.beeple-crap.com/

Fraunhofer FOKUS

The Most Expensive NFTs



69$ Milion

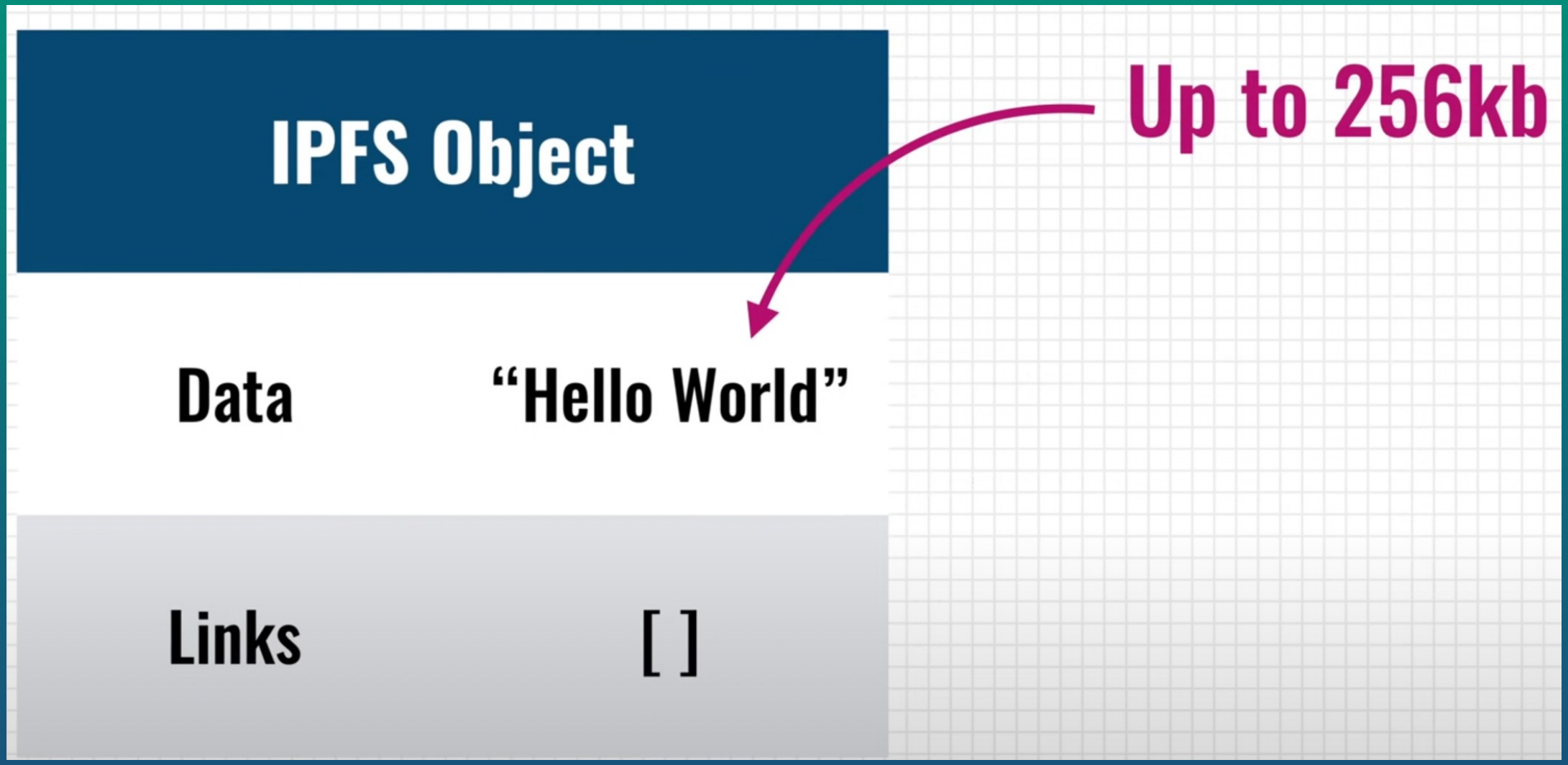
Source: https://www.dezeen.com/2021/03/12/beeple-everydays-nft-christies-auction/, https://de.wikipedia.org/wiki/Beeple

Fraunhofer FOKUS

Distributed File Storage

Fraunhofer FOKUS

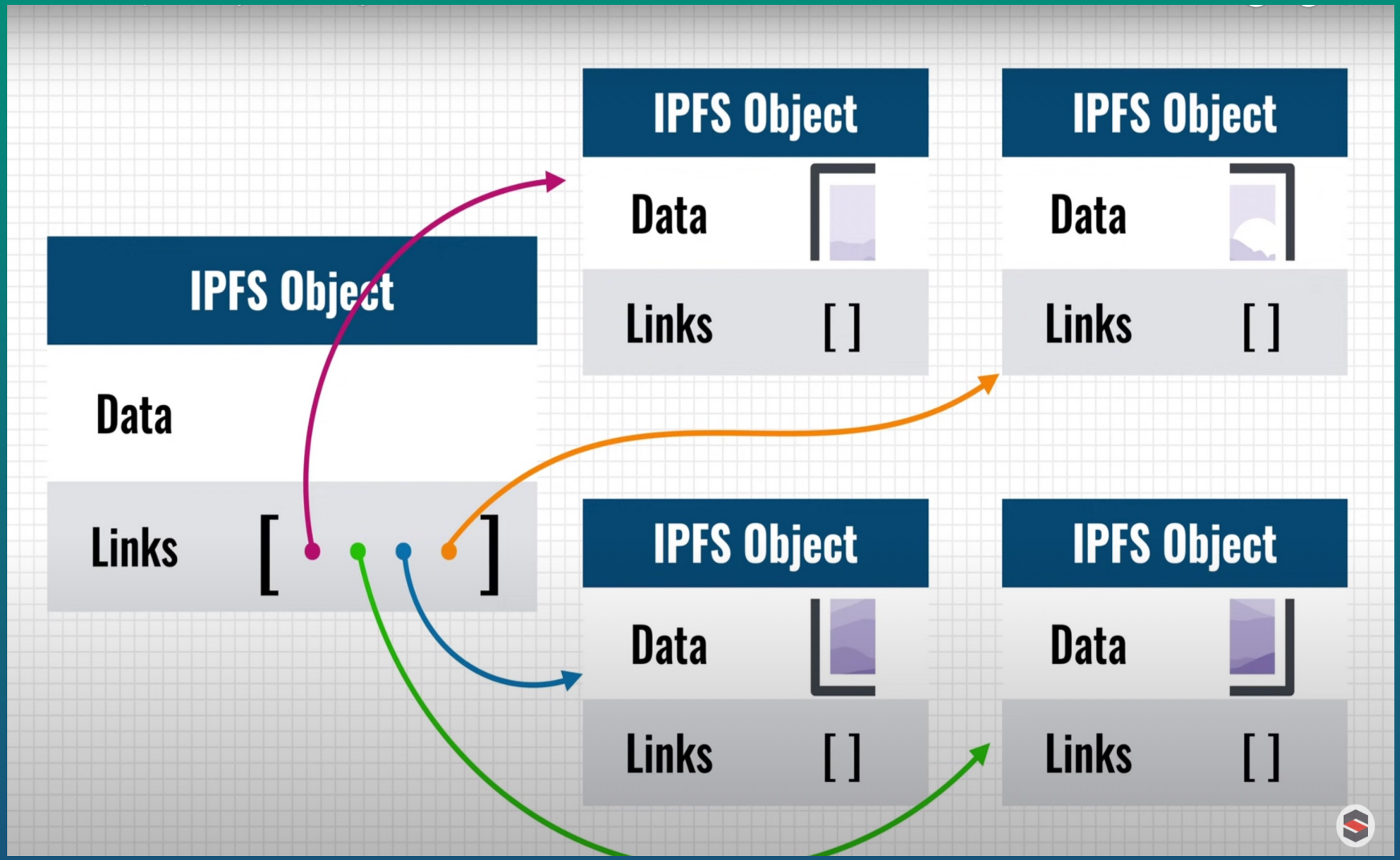
Interplanetary File System



Source: https://www.youtube.com/watch?v=5Uj6uR3fp-U

Fraunhofer FOKUS

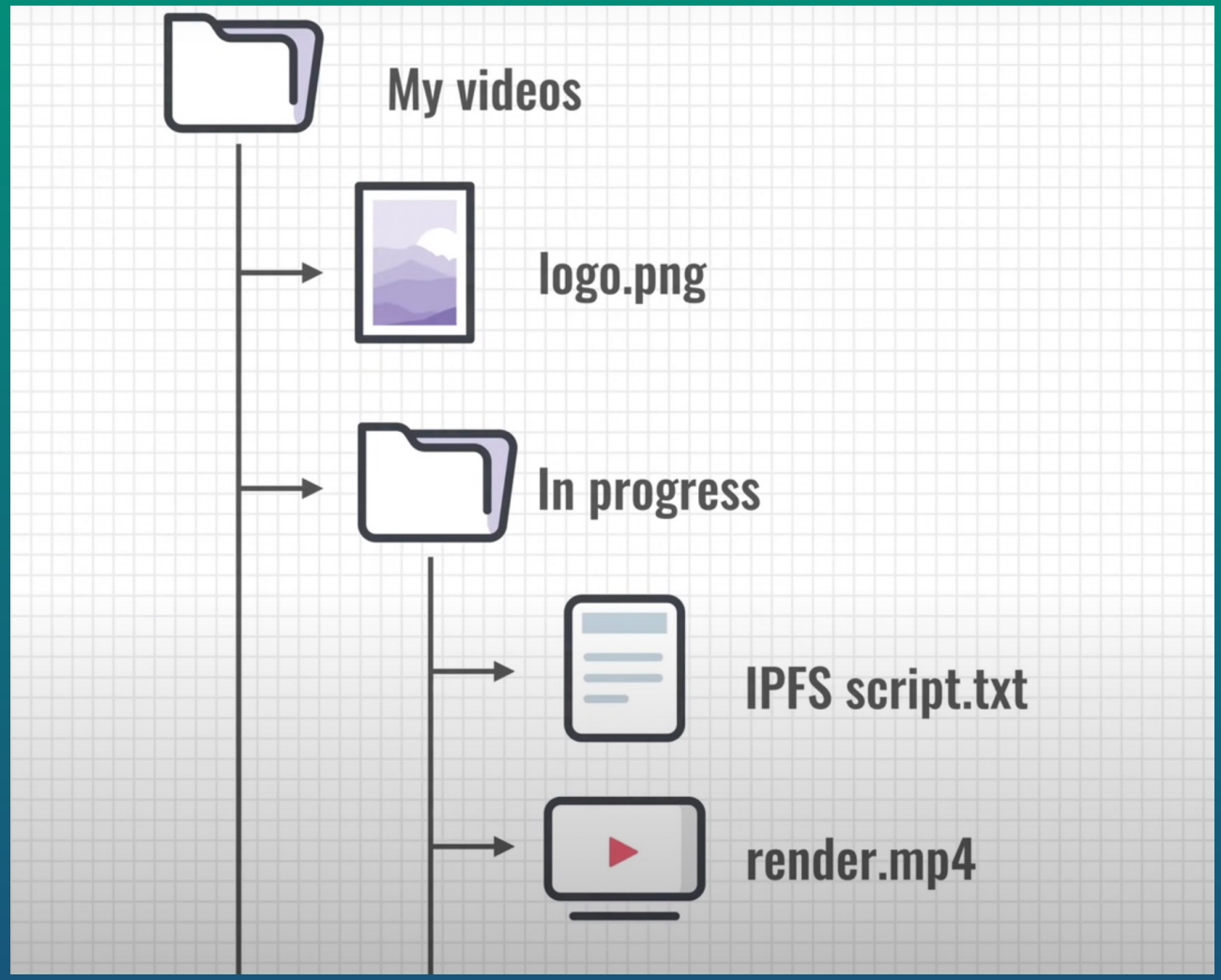
Interplanetary File System



Source: https://www.youtube.com/watch?v=5Uj6uR3fp-U

Fraunhofer FOKUS

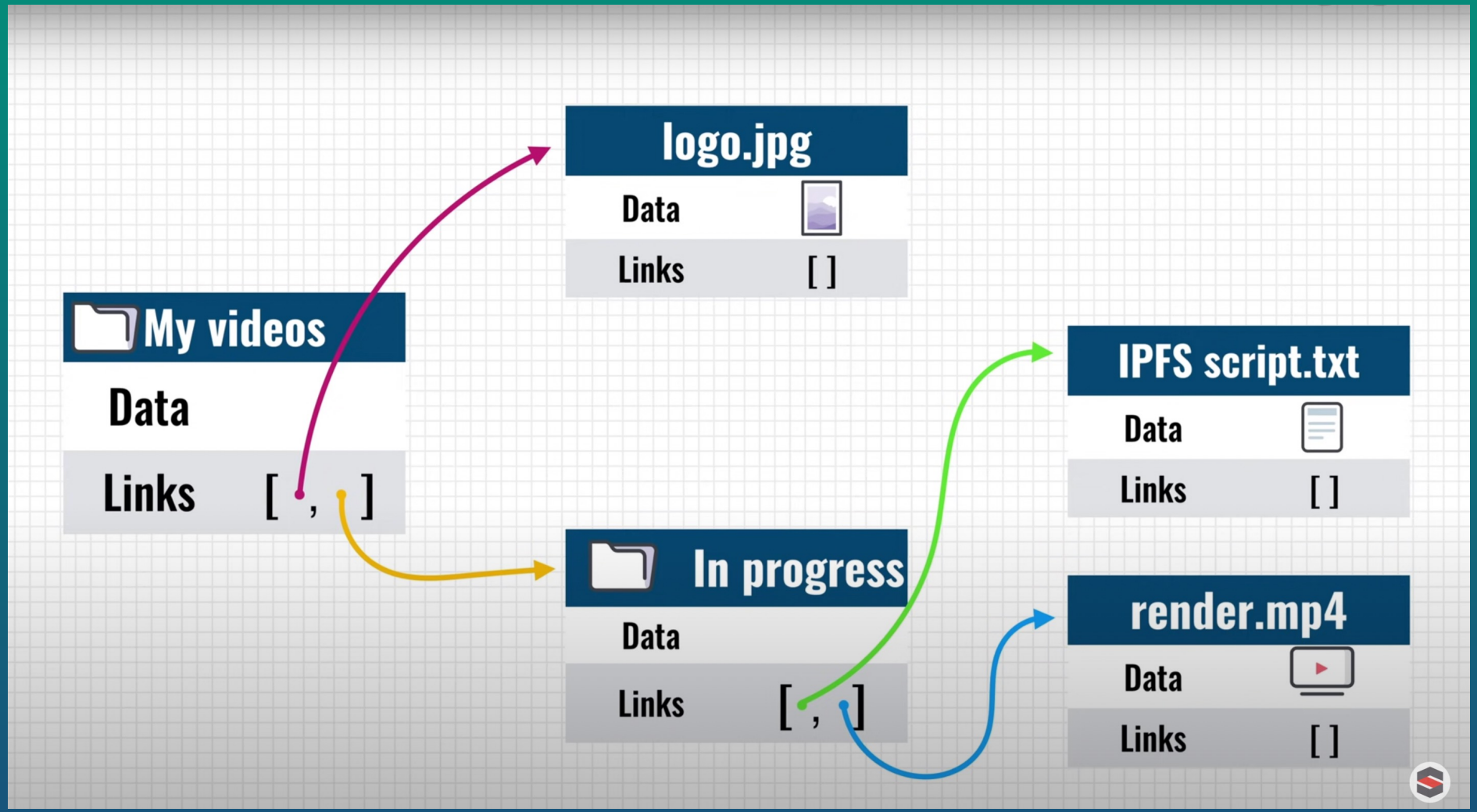
Interplanetary File System



Source: https://www.youtube.com/watch?v=5Uj6uR3fp-U

Fraunhofer FOKUS

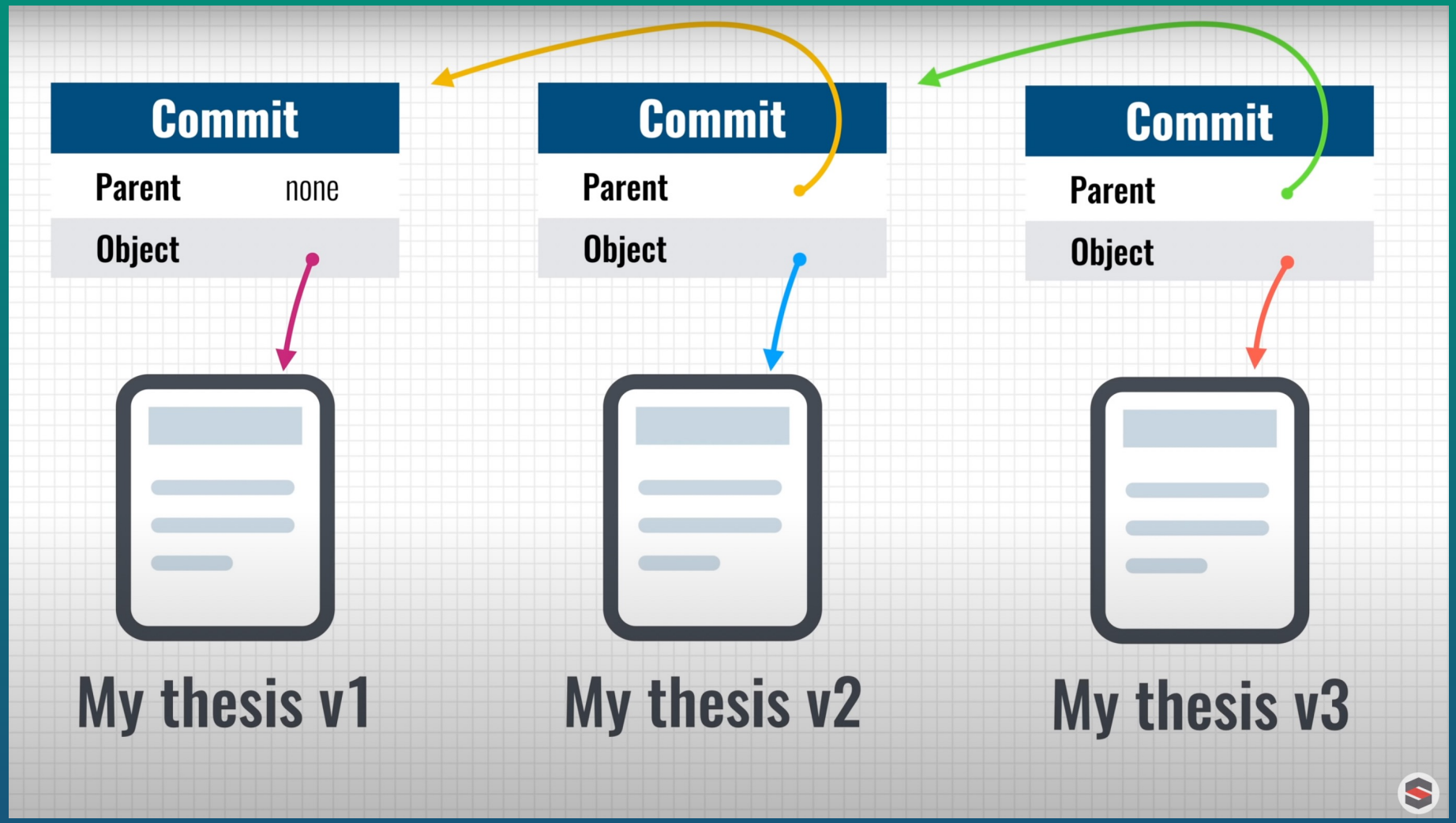
Immutable Datastore like a Blockchain



Source: https://www.youtube.com/watch?v=5Uj6uR3fp-U

Fraunhofer FOKUS

Immutable Datastore Like a Blockchain

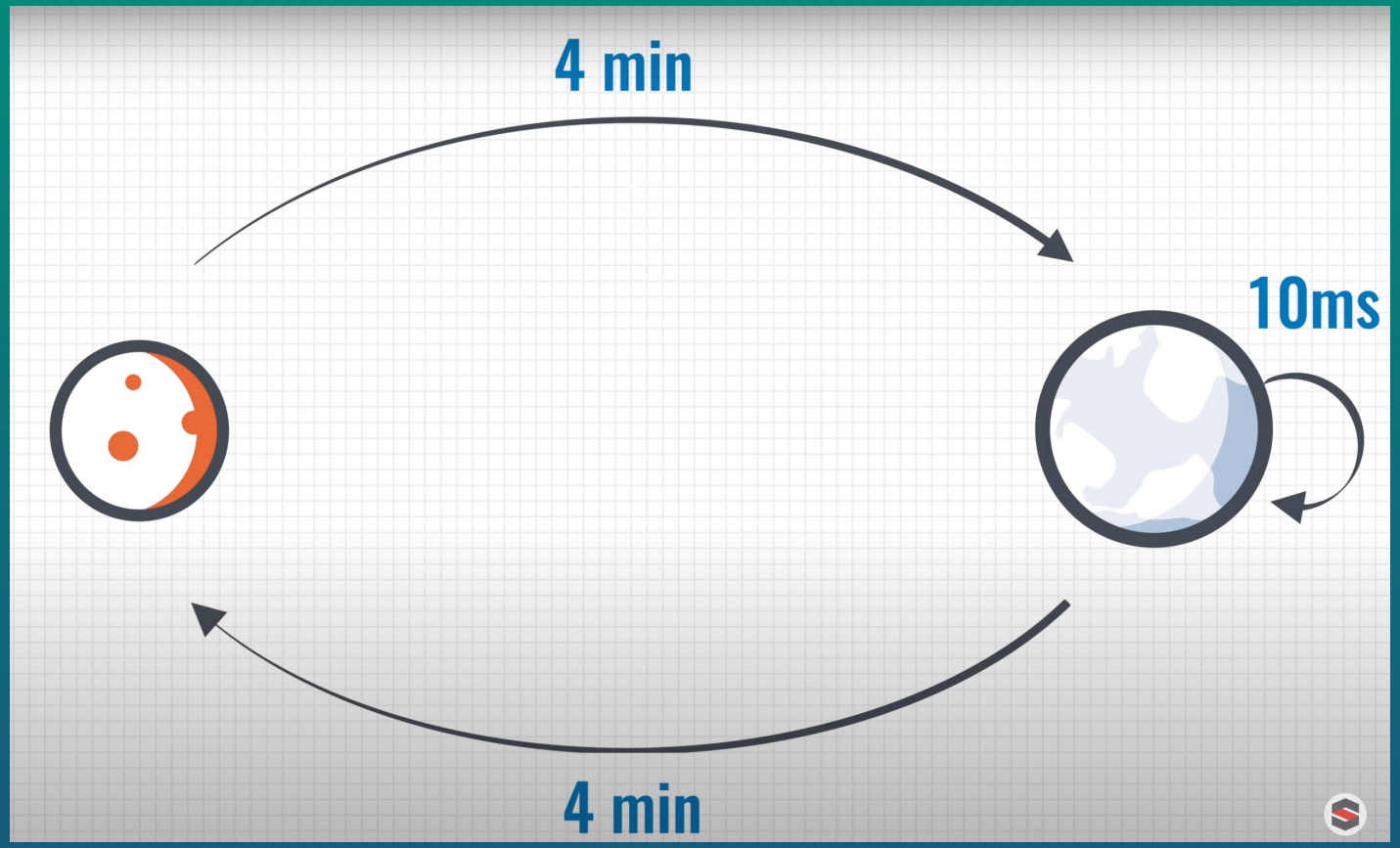


Source: https://www.youtube.com/watch?v=5Uj6uR3fp-U

Fraunhofer FOKUS

Why - Interplanetary

- ✓ Serving a file from mars:
  - ✓ Over Internet min 8 minutes
  - ✓ Over IPFS instantaneously
    - ✓ Because it can be cached



Source: https://www.youtube.com/watch?v=5Uj6uR3fp-U

Fraunhofer FOKUS

Securing Value of Digital Art

Fraunhofer FOKUS

Problems With Digital Media

- Original can be stolen by a hacker
- What if viewer makes a photocopy?
- How to safely sell or rent it?
- Can we verify its authenticity?

Source: https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/posting-film-clips-is-the-new-trend-among-cinegoers/articleshow/70497190.cms

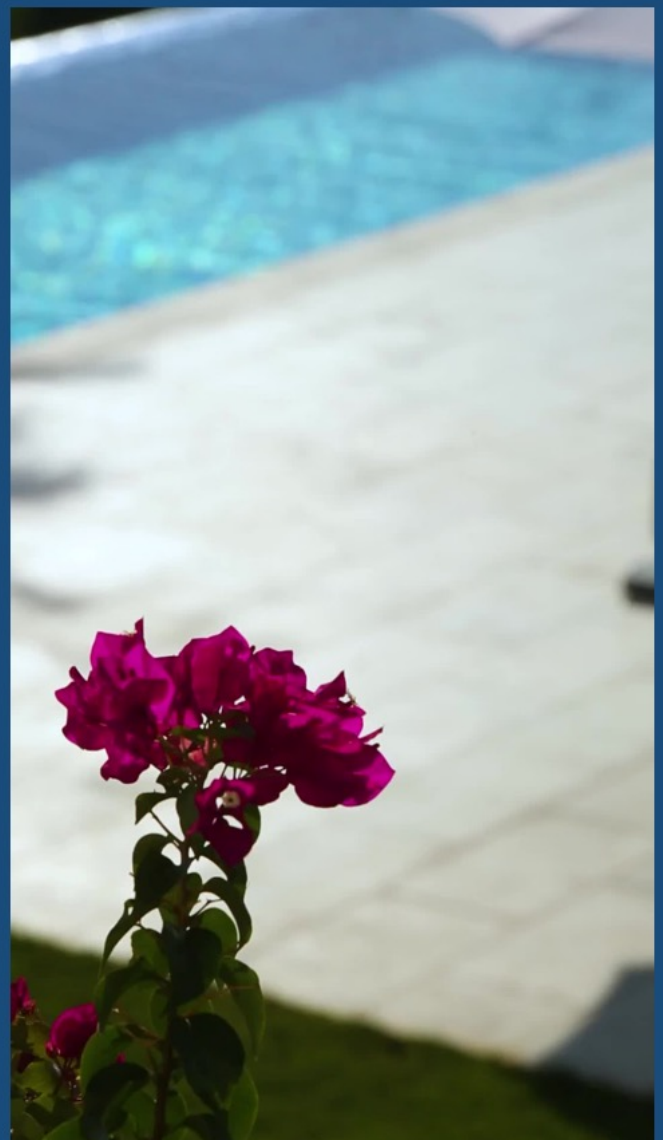
Fraunhofer Digital Uniqueness Platform – Functionality

- Embedding imperceptible identifier into media after uploading it to the platform
- Being able to read the identifier by scanning(photographing) the media with a specific app
- Blockchain based platform, storing transactions about user operations
  - ✓ Adding a media to the platform
  - ✓ Changing the owner of meida etc.
- The original media file is encrypted and never leaves the platform
  - ✓ Only media with embedded identifier can leave the platform
  - ✓ It is rather hard to remove the identifier without destroying the media file

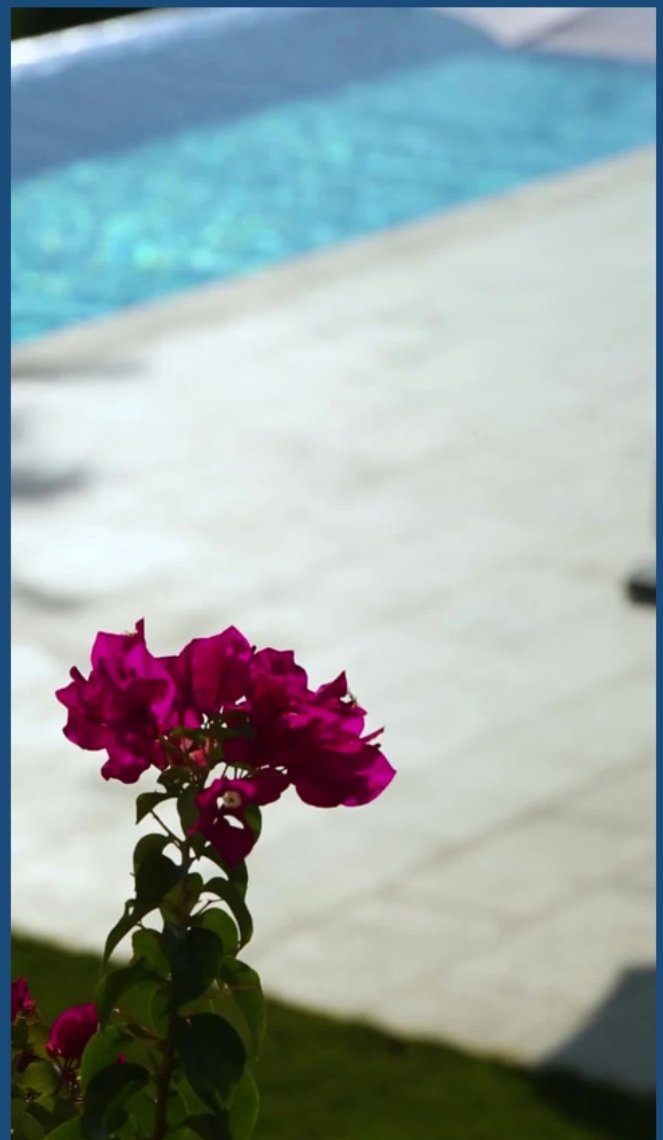
Fraunhofer Digital Uniqueness Platform – Application Area

- Artists and technology professionals who came together to make digital art and content unique
- The marketplace for unique digital art
- Connecting artists, museums, collectors and fans
- The marketplace delivers a trusted channel to buy, rent and sell unique digital imagery
- NFT and uniqueness recognition technology to ensure authentic and secured value for digital transactions

Steganography: How to embed tokens in media?

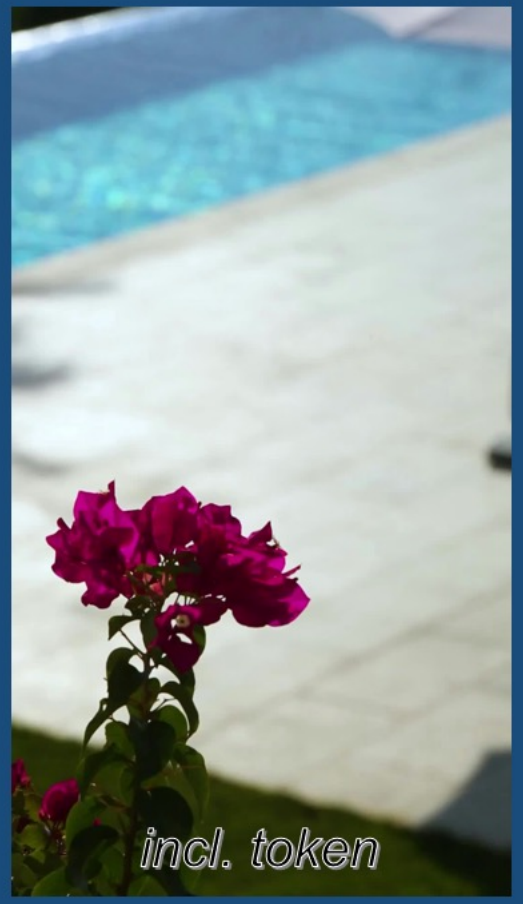


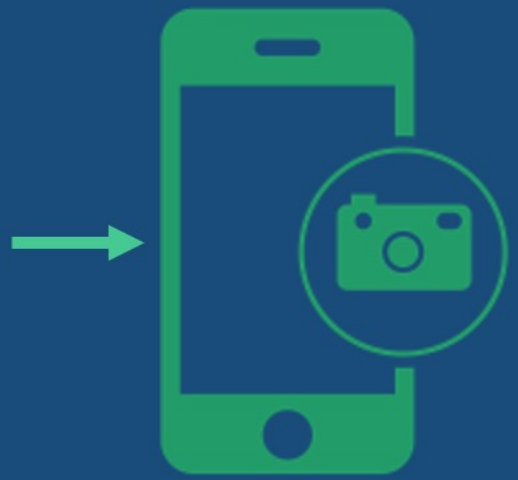
+ Token =



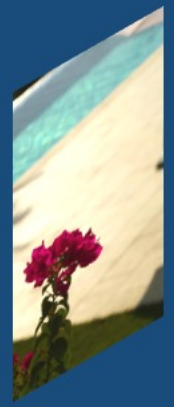
Fraunhofer

Steganography: How to extract tokens from captured media?





Camera



Manipulated Media

Decoder

message

Fraunhofer

Verification of Authenticity of Physical Products

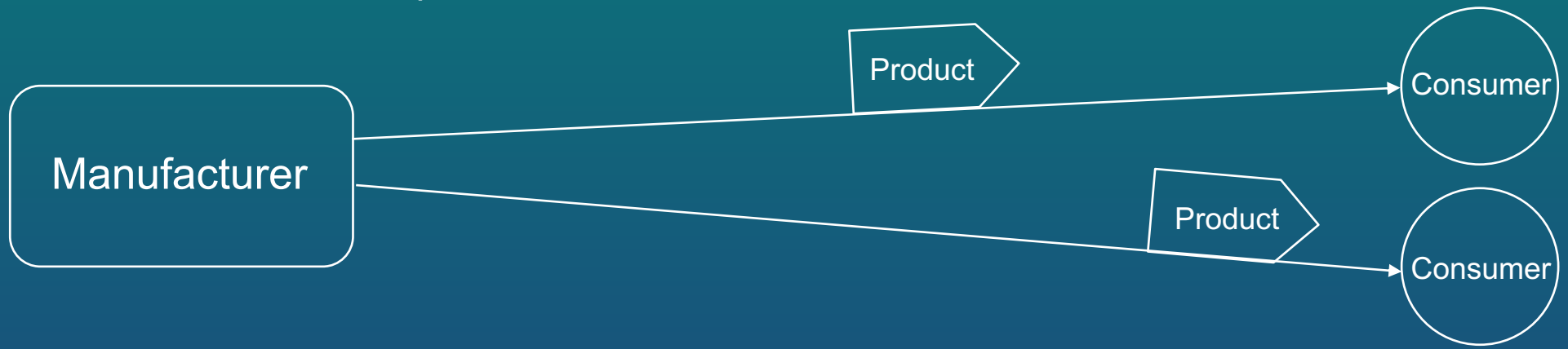
Fraunhofer FOKUS

SmartID in a nutshell - Application Area

- After manufacturer seals a product it travels long way to ist consumer

- During such a long journey things can go wrong
  - ✓ Illegal duplicates of product
  - ✓ Similar looking product with different quality

- How do we make sure the product that is delivered to consumers is authentic
  - ✓ Is it the exact same product from the manufacturer it claims to be?



Fraunhofer FOKUS

SmartID in a nutshell - Functionality

- Marking a product with unique identifier
  - Technique to mark products
  - Integrated it into existing Track & Trace
- Printing the identifier
  - QR codes on product packaging
  - DataMatrix-Codes
  - ISO certified other barcodes
- Being able to read the identifier
  - Online recognition
  - Offline recognition

Source: https://previews.123rf.com/images/artinspiring/artinspiring1701/artinspiring170100371/70266172-qr-code-mit-dem-smartphone-scannen-mobile-scan-app-zum-online-lesen-von-informationen-%C3%BCber-orte-oder.jpg

Fraunhofer FOKUS

Summary of what has been presented

Fraunhofer FOKUS

Summary

- Motivation
- Distributed Knowledge
  - ✓ Blockchain Technologies
  - ✓ Distributed File Storage
- Application Areas
  - ✓ Securing Value of Digital Art
  - ✓ Verification of Authenticity of Physical Products

Thank you for your attention!

Fraunhofer FOKUS
Institute for Open Communication Systems

Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
info@fokus.fraunhofer.de
www.fokus.fraunhofer.de

Contact

Andy Neparidze

andy,neparidze@fokus.fraunhofer.de

Fraunhofer FOKUS