Cryptocurrencies, Blockchain Technologies & the Law

University of Houston Law Center
Prof. Charles D. Brown

Fall 2022

WEB 3
LAW CENTER

Introduction to Class

What have I gotten myself into?

Hello World! - Personal Introduction

Class Syllabus - Aspirational, Flexible, Fiction

Class Structure - Quiz, Technology, New News, Participatory Lecture

Assessments - 25% Quiz, 25% Participation, 50% Written Assessment

Participation - New News, Class Discussions, Prepared on Readings

Written Assessment - “Add something meaningful to the understanding or direction of Web3 law.”

Group or Solo, Practical or Academic, Published or Presented (or Both)

My Web3 Story

Class Introductions

WEB 3
LAW CENTER

Next: What is a blockchain?

Background and Technological Primer

Reading Assignment: FW Chap. 1 & 2

Industry Assignment: Find some method of staying current with the state of the blockchain space. Some ideas include Google Alerts, Twitter follows, Apple News Interests. Read a few articles and be prepared to discuss with the class.

You should be able to explain what makes blockchain unique and why those unique characteristics are so important.

WEB 3
LAW CENTER

Quiz

https://www.medmalfirm.com/quiz/blockchain

WEB 3
LAW CENTER

Housekeeping

I will be out of town for the week of September 19th. We will have a guest lecturer (Susan Lindberg) who will cover SEC securities regulation and NFTs.

Assignment:

Sections 3 and 5 from

https://www.americanbar.org/content/dam/aba/administrative/business_law/buslaw/committees/CL620000pub/digital_assets.pdf

WEB 3
LAW CENTER

Housekeeping

Securities (9-19):

SEC v. W.J. Howey Co., 328 U.S. 293 (1946).

In the Matter of Erik T. Voorhees, File No. 3-15902, Release No. 9592 (June 3, 2014) https://www.sec.gov/litigation/admin/2014/33-9592.pdf

U.S. Securities and Exchange Commission, Statement on digital asset securities issuance and trading (Nov. 16, 2018) https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading

L. Schneider, Oranges are not securities and neither is SOL, Crowdfund Insider (July 12, 2022) https://www.crowdfundinsider.com/2022/07/193572-oranges-are-not-securities-and-neither-is-sol/

NFTs (9-21):

W. Entriken, D. Shirley, J. Evans, N. Sachs, EIP-721: Non-Fungible Token Standard (Jan. 24, 2018) https://eips.ethereum.org/EIPS/eip-721

D. Van Boom, Seth Green Loses $200K Bored Ape Yacht Club NFT in Phishing Scam, CNET, May 18, 2022. https://www.cnet.com/personal-finance/seth-green-loses-200k-bored-ape-yacht-club-nft-in-phishing-scam/ See also story in Wired, https://www.wired.com/story/seth-green-bored-ape-nft-stolen/

Global Blockchain Convergence, A “Sensible” Token Classification System,

available at https://novuminsights.com/post/sensible-token-classification-system/

WEB 3
LAW CENTER

Tech Note

Discord

Discord is a communications platform that serves as the default community manager for most NFT/DAO projects.

The Web3 Law Center is just now starting a discord server. Please follow the link, create an account, and join the Web3LC server.

https://discord.com/invite/AC8BceyU

WEB 3
LAW CENTER

News Note

Alphabet (Google) Invests $1.5 Billion in 4 NFT/Crypto Companies

Fireblocks

Dapper Labs

Voltage

Digital Currency Group

What does an investment of this size tell us about the future of this technology? Keep in mind, they spent between $400 and $800 million on Google Glass.

WEB 3
LAW CENTER

What is a blockchain?

WEB 3
LAW CENTER

What is a blockchain?

Background and Technological Primer

Blockchains are decentralized databases, maintained by a distributed network of computers.

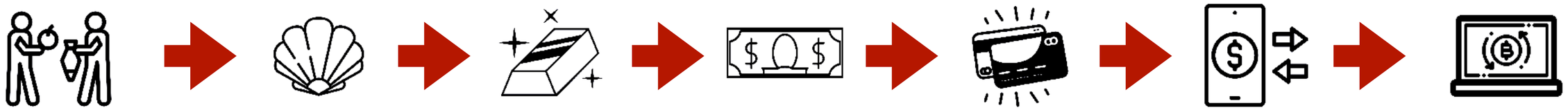
What is a database?

What is a computer?

WEB 3
LAW CENTER

What is a blockchain?

What is money?



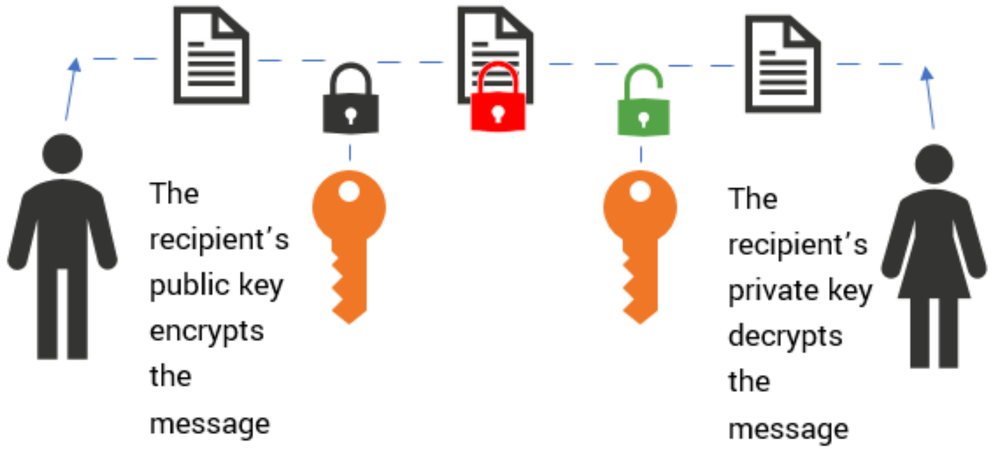
Tangible	→	Less Tangible
Anonymous	→	?
Free Movement	→	?

WEB 3
LAW CENTER

What is a blockchain?

The Encryption Side of Things

1976 - Public-Private Key Cryptography created a way around the shared key problem. Key-pair algorithms create authentication mechanisms that allow that are very, very difficult to break. Diffie and Helman's paper calls for the need for an open hashing model.



1989 - Ron Rivest developed the MD2 algorithm in 1989 it was the first to be widely used in open standards. One-way encryption. Takes a data string and converts it into a fixed string.

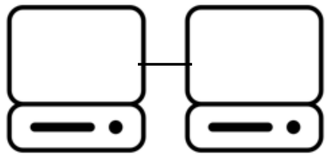
I love my dog. = BE6094D4C12DCE046608FA51F6A9158A
I love my dog! = BB0E53B3B3FE934D83BA8C87690CC7A4
My dog loves my wife. = ECDC4B093451417BE7E1440E36F9B490

WEB 3
LAW CENTER

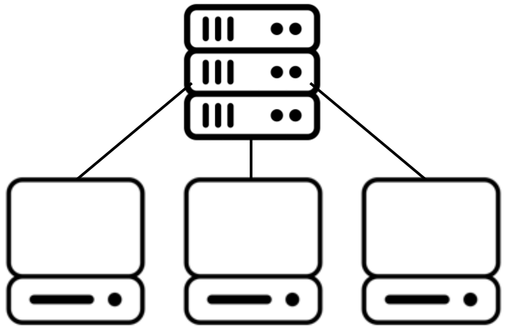
What is a blockchain?

Computer Networking

Pre-1964 - Computers lived alone. While there was terminal access, the computer was an isolated machine.



In August 1964, packet switching technology lays ground work for DARPA and later the internet. The goal was to protect information in the event of nuclear war.



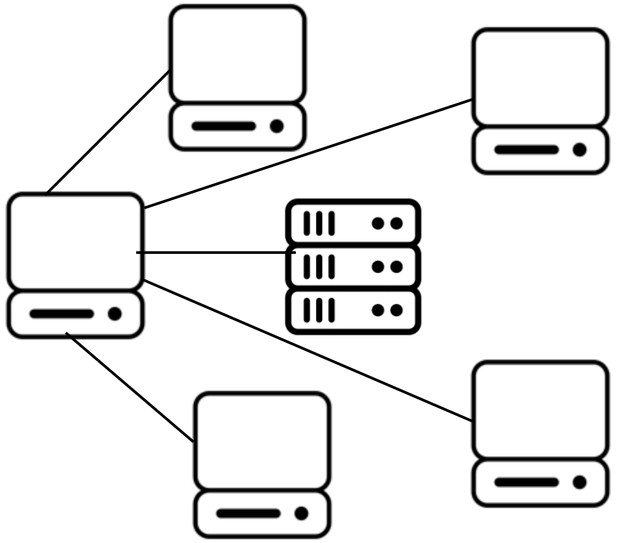
By the mid-1990s DARPA had evolved to become the commercial internet. Web 1.0 Under this client-server model, people went to websites and interacted with the pages served up by the web server. Here, the content creator owned the information, but the information is centralized and therefore vulnerable to security breakdowns, tech breakdowns, and censorship. Whether Google, Amazon, or the New York Times, Web 1.0 websites create content, own the content, and distribute that content (search results, stores, or news).

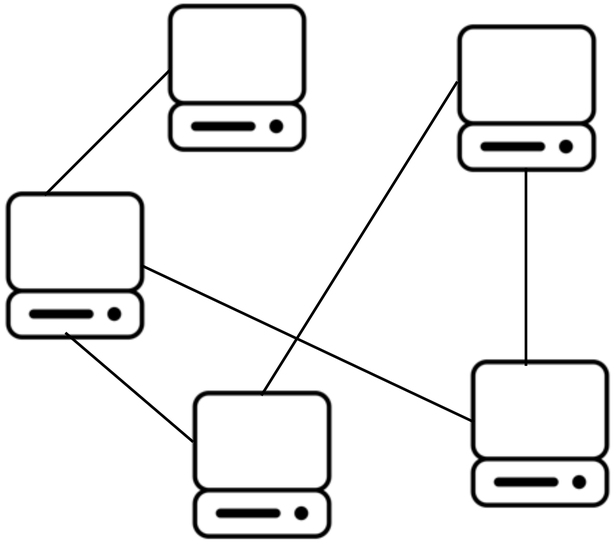
WEB 3
LAW CENTER

What is a blockchain?

Computer Networking

1999 - Napster introduces the world to peer-to-peer file sharing. Each computer acts as a node in the network and contains pieces of files that it serves up based on the file index contained on Napster's servers. Music copyright holders were not thrilled with the new technology, so they fight Napster, keying on the server.





2001 - After Napster pays the price for having a centralized index, BitTorrent and others distribute the index as well for a fully distributed file sharing system. Copyright holders are helpless. There is no one server to shut down. Distribution is now entirely global and decentralized.

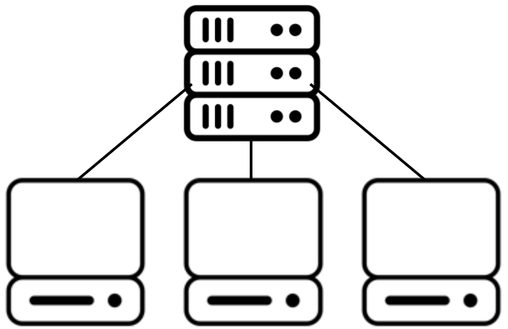
WEB 3
LAW CENTER

What is a blockchain?

Computer Networking

2003 - While the pirates are sharing music, movies, and more, the commercial internet remains in Web 1.0. But in 2003 with MySpace and 2004 with Facebook, the internet begins to change to Web 2.0. Here, the content creator uploads the content to a corporate server and the corporation monetizes it. YouTube, Instagram, Facebook, TicToc, and Yelp. All of these websites take content, monetize it, and pay nothing to the creator.

This consolidates money and power in the hands of those able to create and monetize the network effect.



If you are not paying for it, you're not the customer; you're the product being sold. - Andrew Lewis

WEB 3
LAW CENTER

What is a blockchain?

How do websites actually work?

Websites are viewed by browsers that interpret the computer language that the website is written in.

Client Side v. Server Side

Most of the information on the page is stored in a server-side database. For example, WordPress, the largest Content Management System on the Web.

So the large corporations that drive so much engagement off of other people's content are also capable of storing user information in their private databases and selling that information to others or displaying it (or censoring it) with little regard for the user's wishes.

WEB 3
LAW CENTER

What is a blockchain?

The Backdrop of the Blockchain Movement

The haves v. have nots. 1%ers. 2008 Financial Crisis.

Apple vs. Facebook, Small Business, Instagram, FBI, etc.

Hacking, shared data with 3rd parties, scraping data, invasive ads…

Social backlash, social censoring, opposing viewpoints.

Free speech, free expression, financial restraints.

Meme stocks, NFTs, HODL, and distribution of economic opportunity.

WEB 3
LAW CENTER

Quiz

https://www.medmalfirm.com/quiz/blockchain

WEB 3
LAW CENTER

Housekeeping

Written Assessment

- Mentors
- Tornado Cash and Regulation
- Work with the ADR team and generate work product from that.
- Privacy concerns with USDC and FedNow cash.
- Building an automated RSS feed or news feed for legal topics. Should be accompanied by an explanation of the categories and sources.

WEB 3
LAW CENTER

Tech Note

GitHub

GitHub serves a number of functions for programmers.

1. File Storage - People working on software can store it here and access it from multiple locations with multiple device types.
2. Collaboration - People can access the source code, make changes, and then either continue with their fork or have the changes merged into the main branch.
3. Resume - When programmers want to show their work to potential employers, this is their resume.

What have you used it for?

WEB 3
LAW CENTER

News Note

Tether says it's not Freezing Tornado Cash Addresses Until Government Tells It To

8-8-22 - “Today, Treasury is sanctioning Tornado Cash, a virtual currency mixer that launders the proceeds of cybercrimes, including those committed against victims in the United States.”

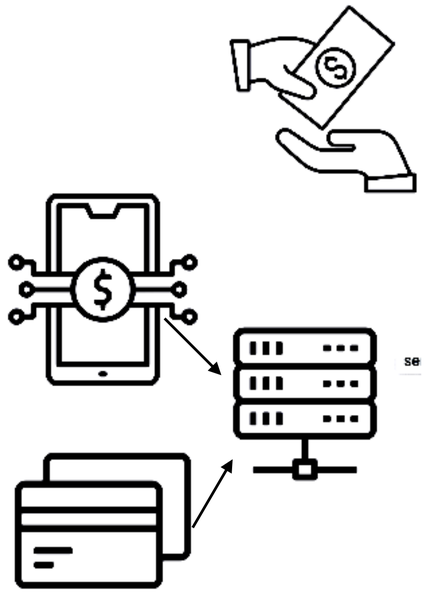
https://www.theblock.co/post/165513/tether-says-its-not-freezing-tornado-cash-until-government-tells-it-to

https://coincenter.substack.com/p/how-does-tornado-cash-actually-work?utm_source=substack&utm_medium=email

WEB 3
LAW CENTER

What is a blockchain?

Digital Currency and the Problem of Double Spending



If I buy something with cash, I cannot spend the same dollar again as it has been given to another person.

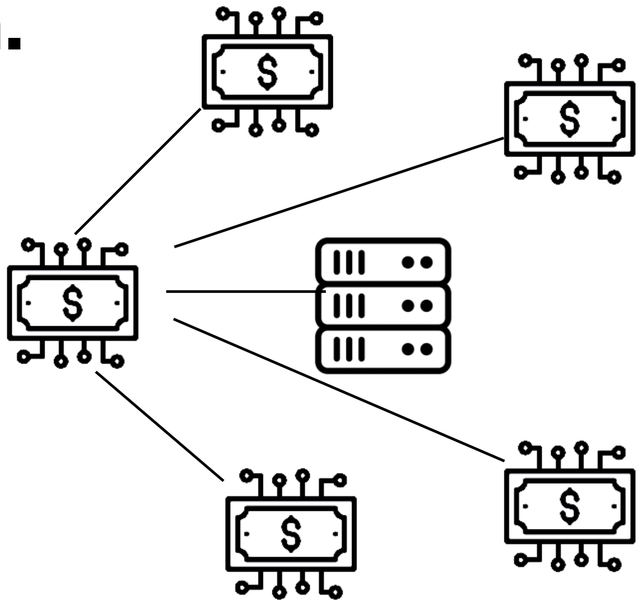
If I use digital currency or a credit card, the transaction must clear a central server (bank or credit card company) to verify funds and complete the transaction.

Without a central server, there is nothing to prevent a buyer from spending the same digital currency to purchase two different items.

WEB 3
LAW CENTER

What is a blockchain?

A blockchain is born. We call it Bitcoin.



In 1994, DigiCash is formed to allow anonymous cash transfers. But the ledger was on one server. Oops.

In 2008, “Satoshi Nakamoto” published a white paper that merged the ideas that we have discussed and, using a concept called blockchain, created a distributed, peer-to-peer cash system using a distributed ledger. Nakamoto called it Bitcoin. In 9 pages, Nakamoto changed the world.

WEB 3
LAW CENTER

What is a blockchain?

The Byzantine General's Problem

Several divisions of the Byzantine army are stationed just outside of an enemy city and are preparing for battle. Various generals can only communicate with each other via a messenger. They must agree upon a common course of action. However, we must assume that some generals are traitors who wish to prevent loyal generals from agreeing upon a common course of action. An algorithm is needed to ensure that a small group of traitors can't disrupt communications. To solve the Byzantine Generals problem, loyal generals need a secure way to come to agreement on a plan (known as consensus) and carry out their chosen plan (known as coordination).

It is very difficult to prove the authenticity of a message without a central coordinating authenticator.

WEB 3
LAW CENTER

What is a blockchain?

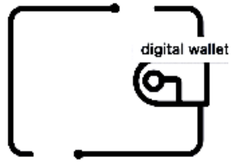
How Bitcoin Creates BFT (Byzantine Fault Tolerance)

They use a proof-of-work chain to solve the problem. The proof-of-work is so difficult, it's expected to take 10 minutes of them all working at once before one of them finds a solution. Once one of the generals finds a proof-of-work, he broadcasts it to the network, and everyone changes their current proof-of-work computation to include that proof-of-work. - Satoshi Nakamoto

WEB 3
LAW CENTER

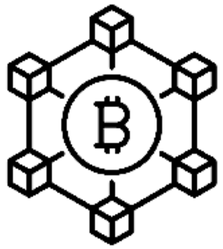
How does a blockchain work?

Perfect trust in an anonymous and hostile environment.



Public-Private Key - Commonly known as a wallet.

Bitcoin is sent from one wallet to another wallet.

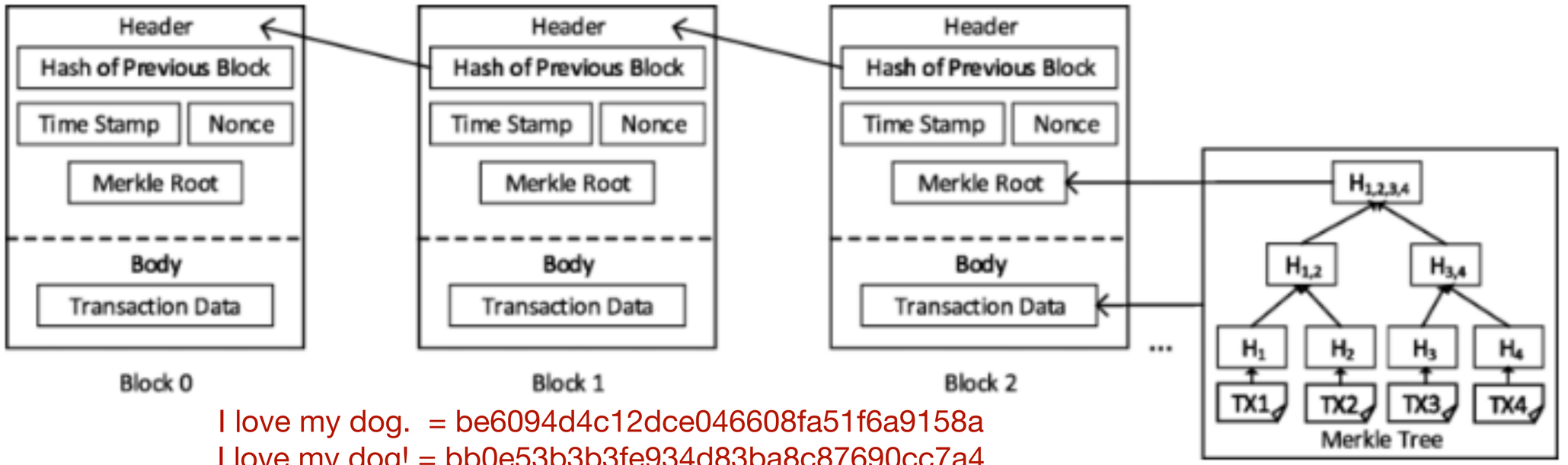


The transaction is validated and the balances in each ledger are edited.

WEB 3
LAW CENTER

How does a blockchain work?

Anatomy of a Block



I love my dog. = be6094d4c12dce046608fa51f6a9158a

I love my dog! = bb0e53b3b3fe934d83ba8c87690cc7a4

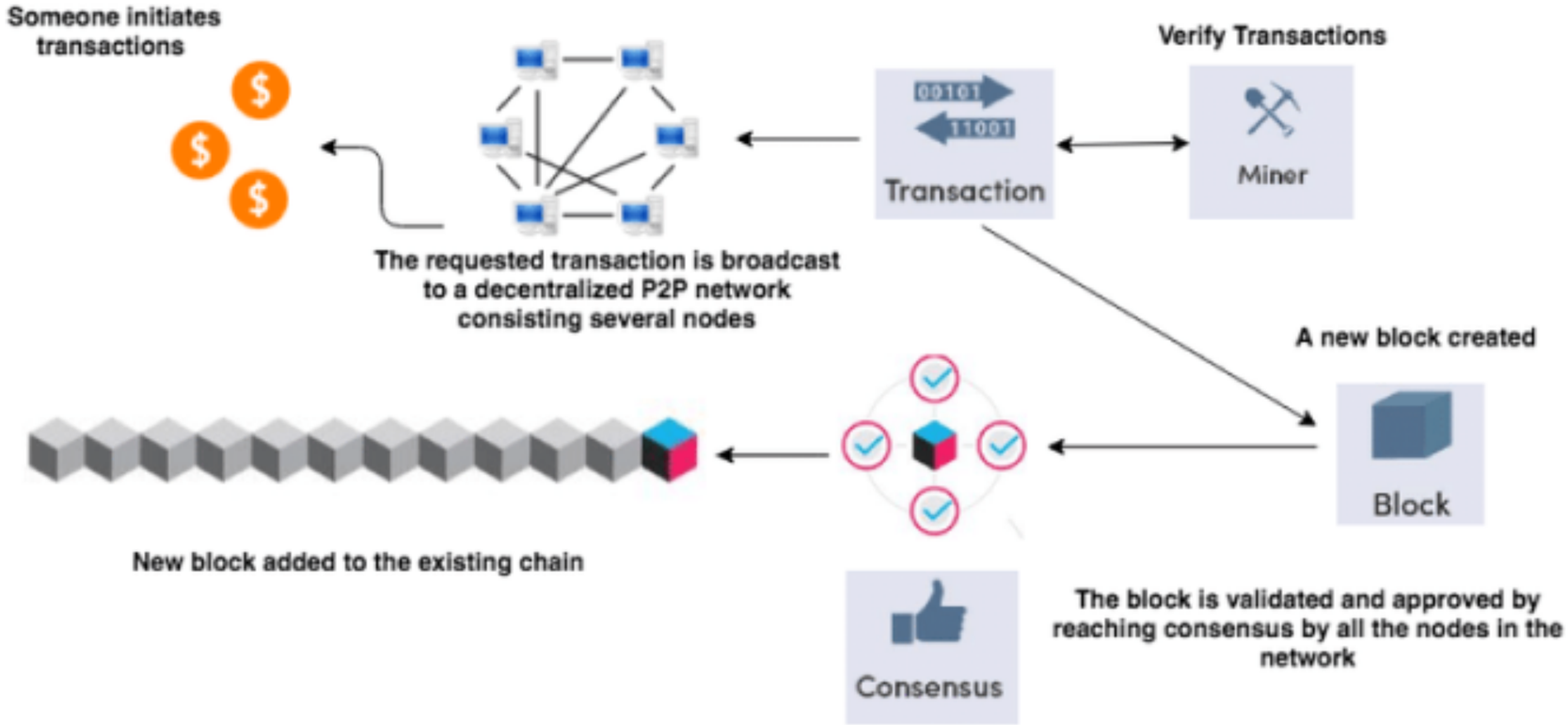
be6094d4c12dce046608fa51f6a9158abb0e53b3b3fe934d83ba8c87690cc7a4 = 3aebd55e6bf738c2c6483ada58dd01b7

Blockchain for Dynamic Spectrum Management - Scientific Figure on ResearchGate.

WEB 3 LAW CENTER

How does a blockchain work?

Nodes, Mining, and Distribution



Functional diagram of a Blockchain network - Scientific Figure on ResearchGate.

WEB 3 LAW CENTER

Characteristics of Blockchain

For better or worse.

Disintermediated.

Transnational.

Resilient.

Resistant to change.

Nonrepudible.

Pseudonymous.

Transparent.

WEB 3
LAW CENTER

Characteristics of Blockchain

For better or worse.

Incentivization and Cost-Structures (PoW, Bounties, Gas)

Consensus (PoW, PoS, Delegated PoS)

Autonomous Software

WEB 3
LAW CENTER

Blockchain Use Cases

What is the point of all of this?

Smart Contracts (with and without an Oracle)

Transaction Register

Store of Value

Bored Apes

Authentication

Democratic Entities

What else?

WEB 3
LAW CENTER

Next: Blockchain as Cryptocurrency

Background and Technological Primer

Reading Assignment: FW Chap. 3

Industry Assignment: Find a couple of good explanations of how blockchain works as a currency. The goal is to put together a library from reputable sources that meet people at multiple entry points. These links will be entered on the quiz sheet.

By the end of the next section, you should have an understanding of how blockchain technology is used to create a “currency.”

WEB 3
LAW CENTER

Quiz

https://www.medmalfirm.com/quiz/blockchain

WEB 3
LAW CENTER

Housekeeping

Assorted

- Work with the ADR team and generate work product from that.

- Pick one of the agencies that regulate blockchain items and describe the history, legal source, scope, and powers of that agency.

- Syllabus changes

- Email addresses - I sent the syllabus change to email, discord, and GitHub. In the future, I will just be updating GitHub.

- https://www.coindesk.com

-NFTs

WEB 3
LAW CENTER

Tech Note

GitHub

Join the Web3Law GitHub repository (https://github.com/justcb/web3law).

Download the current files.

Set email notifications.

WEB 3
LAW CENTER

News Note

Binance Froze Russian Gun Maker's Crypto Assets, Amid Ukrainian Pressure

Binance, the world’s largest crypto exchange by volume, froze a wallet related to Vladislav Lobaev, a Russian gun manufacturer who raised funds for the country's troops in Ukraine, according to a Lobaev representative and blockchain data analysis.

While the Ukrainian government did not mention Lobaev or anyone else by name, last week the Security Service of Ukraine (SSU) published a press release saying the agency “blocked a crypto wallet belonging to a Russian citizen who is sponsoring Russian war in Ukraine.” CoinDesk has confirmed that the wallet was Lobaev’s Binance account.

https://www.coindesk.com/layer2/sinweek/2022/08/31/binance-froze-russian-gun-makers-crypto-assets-likely-at-ukraines-request/

WEB 3
LAW CENTER

Blockchain as a cryptocurrency.

WEB 3
LAW CENTER

Cryptocurrency as a Payment System

- What is a payment system and why do we need it?
- What is a remittance?
- Current payment systems like banks, Western Union, PayPal can be expensive and/or have significant delays.
- How could Bitcoin overcome some of these issues?

WEB 3
LAW CENTER

Cryptocurrency as a Payment System

Bitcoin's advantages as a payment system.

- Bitcoin is international.
- Bitcoin is trustworthy.
- Bitcoin is pseudonymous.
- Bitcoin is decentralized.
- Once the transaction occurs, Bitcoin is essentially permanent.
- Bitcoin is relatively efficient and essentially instantaneous.
- Bitcoin is platform independent.

WEB 3
LAW CENTER

Cryptocurrency as a Payment System

Bitcoin's dangers as a payment system.

- Bitcoin is international.
- Bitcoin is trustworthy.
- Bitcoin is pseudonymous.
- Bitcoin is decentralized.
- Once the transaction occurs, Bitcoin is essentially permanent.
- Bitcoin is relatively efficient and essentially instantaneous.
- Bitcoin is platform independent.

WEB 3
LAW CENTER

Cryptocurrency as a Payment System

Balancing Security and Freedom

Security

The government must have information about the flow of money to prevent money laundering, terrorist financing, and enforce criminal penalties and sanctions.

Freedom

If the government has information about the flow of money, it will inevitably use that information to restrict activities that it disagrees with.

WEB 3
LAW CENTER

Cryptocurrency as a Payment System

Balancing Security and Freedom

Security

People are scary.

Freedom

The government is scary.

WEB 3
LAW CENTER

Cryptocurrency as a Payment System

Balancing Security and Freedom

Security

We trade away some, if not much, of our freedom for the feeling of safety that comes with sticking with what we know because the known can only be as scary as it already is, whereas the unknown has limitless potential to be terrifying. - Philip K. Jason

Freedom

"Of all tyrannies, a tyranny sincerely exercised for the good of its victims may be the most oppressive. It would be better to live under robber barons than under omnipotent moral busybodies. The robber baron's cruelty may sometimes sleep, his cupidity may at some point be satiated; but those who torment us for our own good will torment us without end for they do so with the approval of their own conscience." ~ C. S. Lewis

WEB 3
LAW CENTER

Cryptocurrency as a Payment System

Government vs. Private Sector

Are we comfortable having companies act because of government or societal pressure to do things the government couldn’t do on its own?

WEB 3
LAW CENTER

Quiz

https://www.medmalfirm.com/quiz/blockchain

WEB 3
LAW CENTER

Housekeeping

Assorted

- Work with the ADR team and generate work product from that.

WEB 3
LAW CENTER

Tech Note

Metamask

Metamask wallet is a very common and relatively safe hot wallet that can be used to access blockchain accounts which can include NFTs and cryptocurrencies. It is available for computers and smart phones.

Please download metamask and create a wallet. When you do, you will be given a seed phrase with 12 words. This is very important. Store these words in a safe place. NEVER send them to anyone. With these words, anyone can take over your wallet.

After the merge, we will be minting an NFT. We will discuss how to pay the gas for those who do not own any Eth.

WEB 3
LAW CENTER

News Note

One Way to Stop Mass Shootings

In 2018, after the Parkland shooting, I wrote a series of articles about how credit card companies and banks played a critical role in financing mass shootings — and how they could help prevent these murders, but have thus far decided to look the other way. A majority of shooters use credit and debit cards to acquire their guns, ammunition and body armor — and the companies behind those card networks have a unique vantage point to spot suspicious buying patterns before law enforcement, families or just about anyone else.

A spokesman for Mastercard told me earlier this summer that the company "did not have a say in the decision" on creating a new code.

"Our position remains the same," he added. "The issue of gun violence needs to be addressed and it is the responsibility of elected officials to enact meaningful policies to address this issue."

WEB 3
LAW CENTER

Cryptocurrency and Crime

How is it used and how big of a problem is it?

In my opinion, the best resource for information related to Crypto and Crime is the Chainalysis Crypto Crime Report 2022. It is the source for the following section.

We will discuss criminal acts first, then we will cover money laundering, terrorist financing, and proliferation financing.

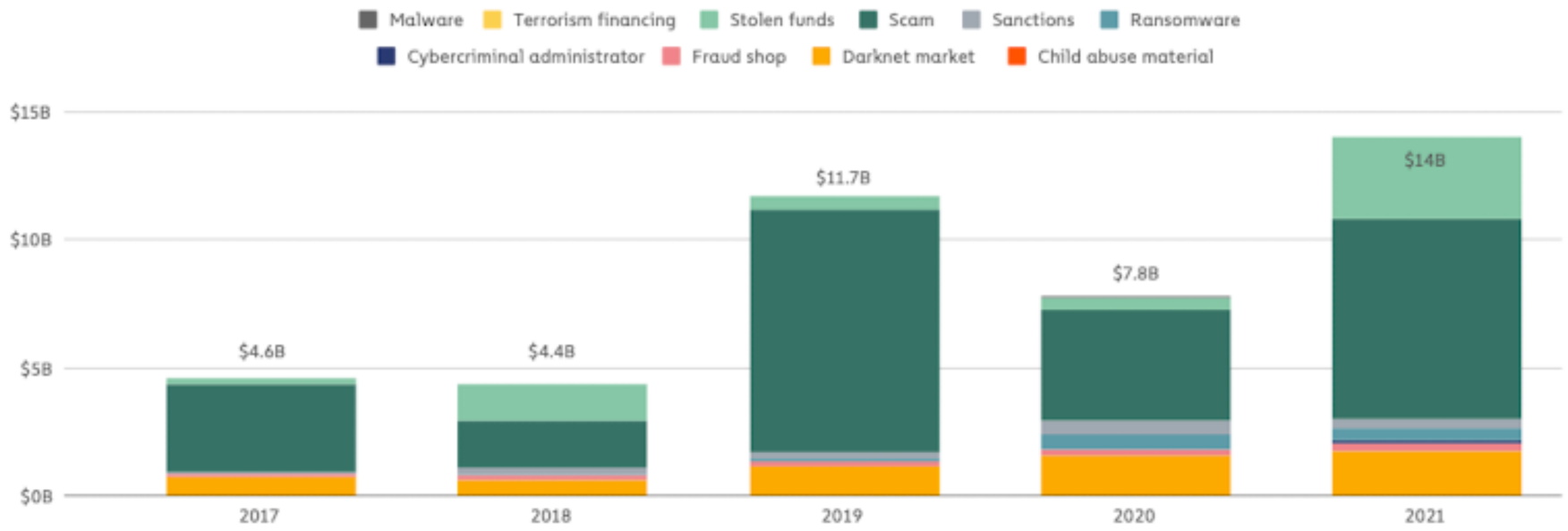
WEB 3
LAW CENTER

Cryptocurrency and Crime

How is it used and how big of a problem is it?

Cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020.

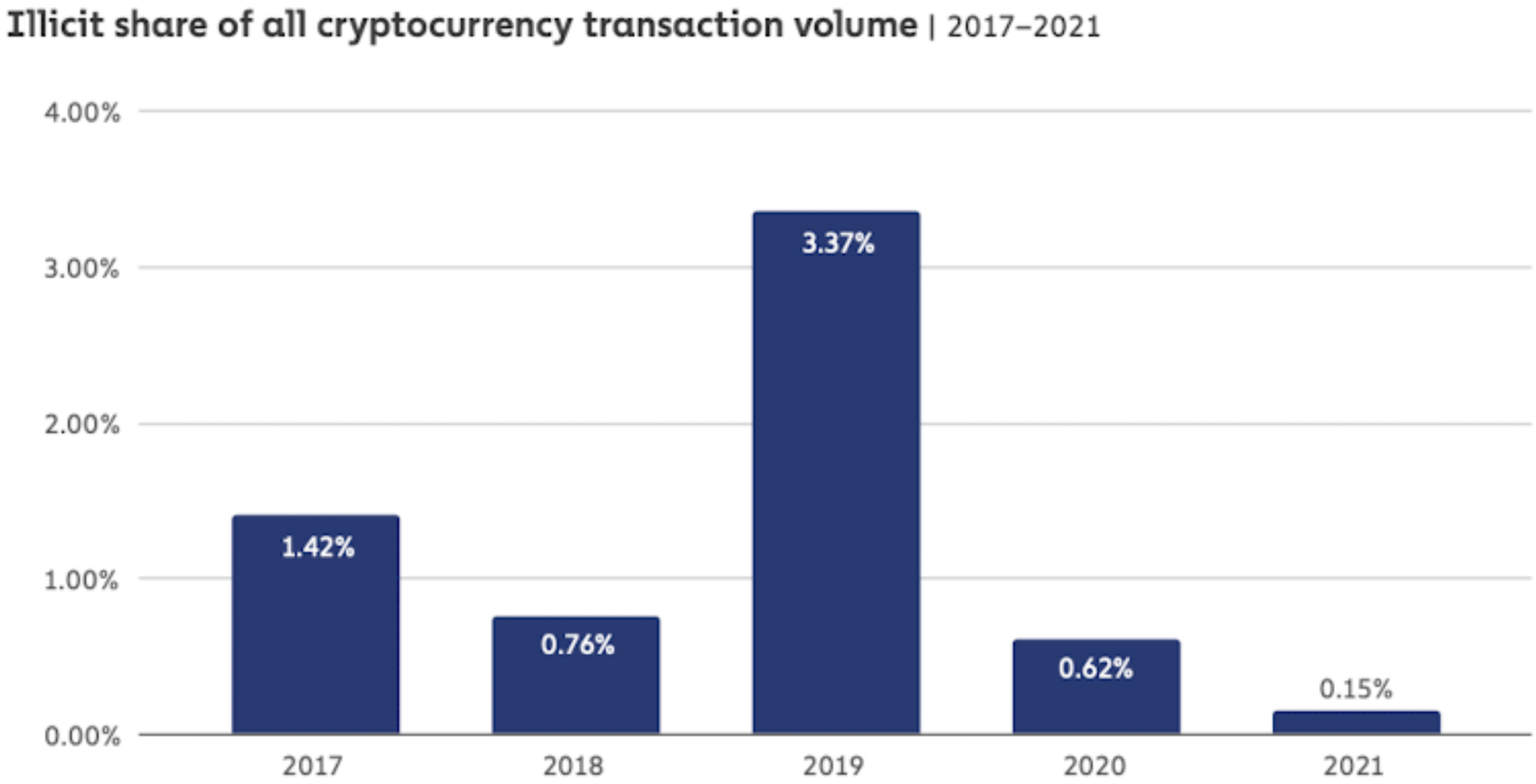
Total cryptocurrency value received by illicit addresses | 2017–2021



WEB 3
LAW CENTER

Cryptocurrency and Crime

How is it used and how big of a problem is it?

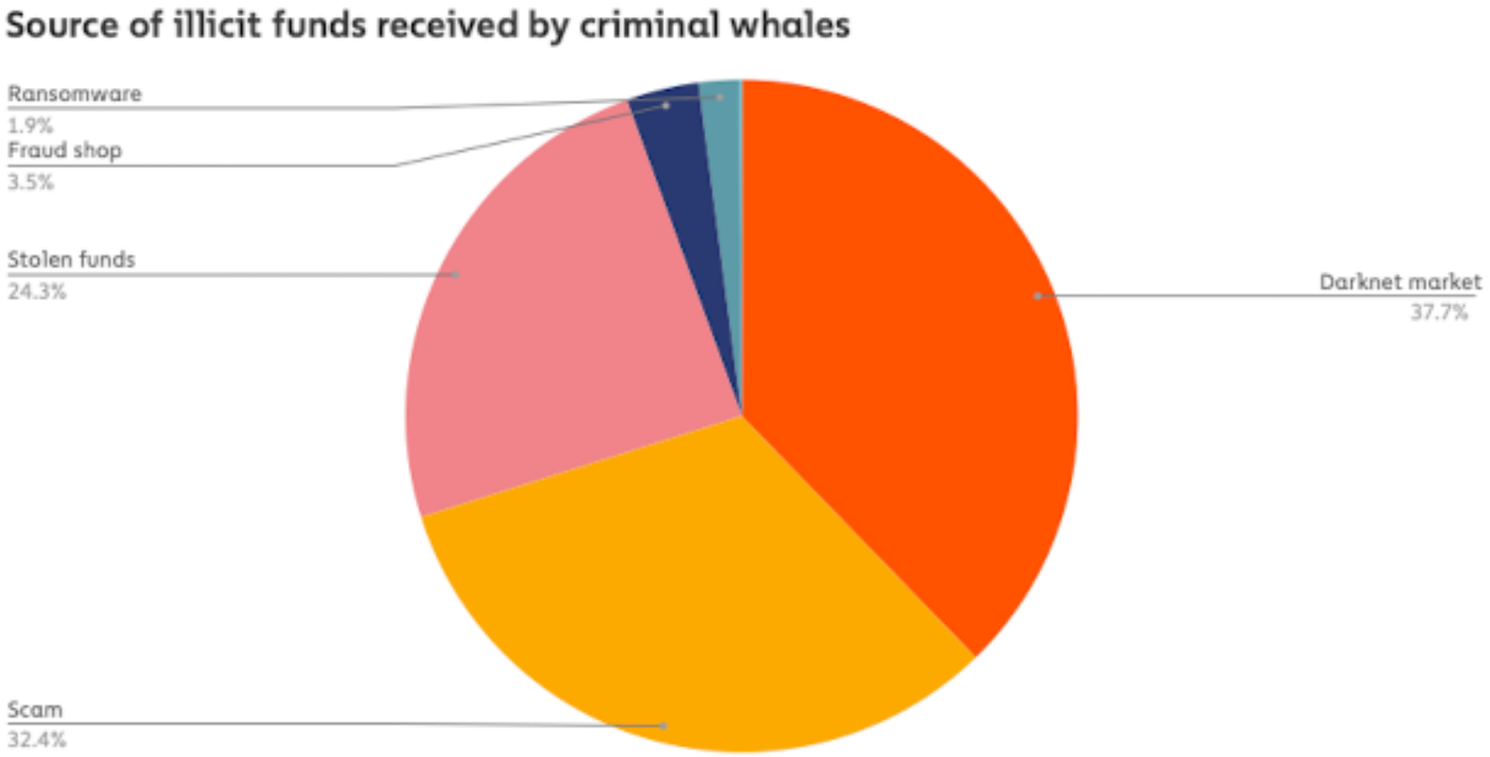


WEB 3
LAW CENTER

Cryptocurrency and Crime

How is it used and how big of a problem is it?

There are 4,068 Criminal Whales
Holding $25 Billion Worth of Currency



WEB 3
LAW CENTER

Cryptocurrency and Crime

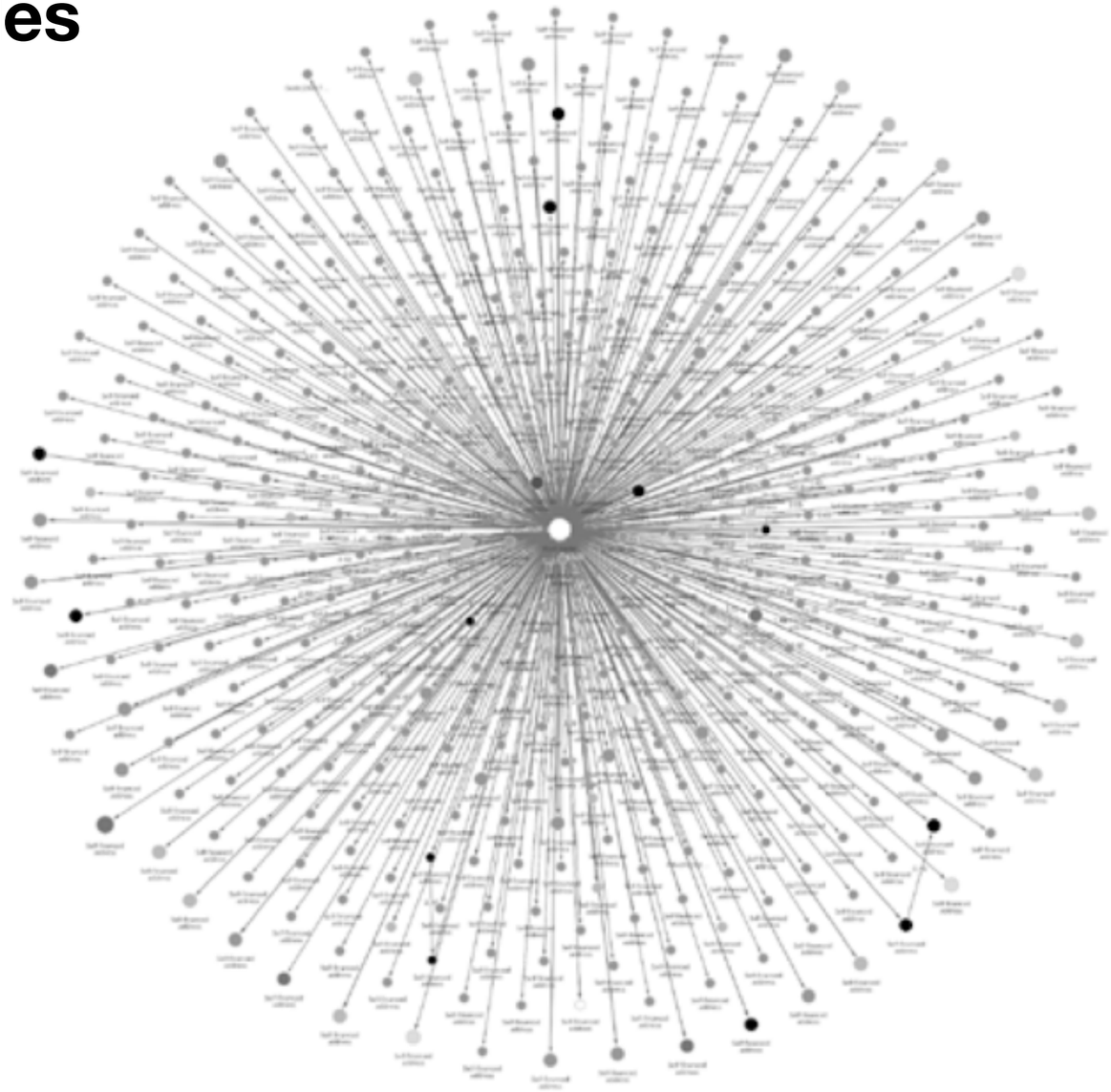
NFTs and Crime

Wash Trades, Rug Pulls, and Money Laundering

WEB 3
LAW CENTER

Cryptocurrency and Crime

NFT Wash Trades



WEB 3
LAW CENTER

Cryptocurrency and Crime

NFT Wash Trades

Wash trader group	Number of addresses	Profits from wash trading
Profitable wash traders	110	$8,875,315
Unprofitable wash traders	152	- $416,984
All	262	$8,458,331

WEB 3
LAW CENTER

Cryptocurrency and Crime

NFT Wash Trades

Is it illegal? Should it be?

WEB 3
LAW CENTER

Cryptocurrency and Crime

NFT Wash Trades

Is it illegal? Should it be?

WEB 3
LAW CENTER

Cryptocurrency and Crime

NFT Rug Pulls

What is it? Is it illegal?

WEB 3
LAW CENTER

Cryptocurrency and Crime

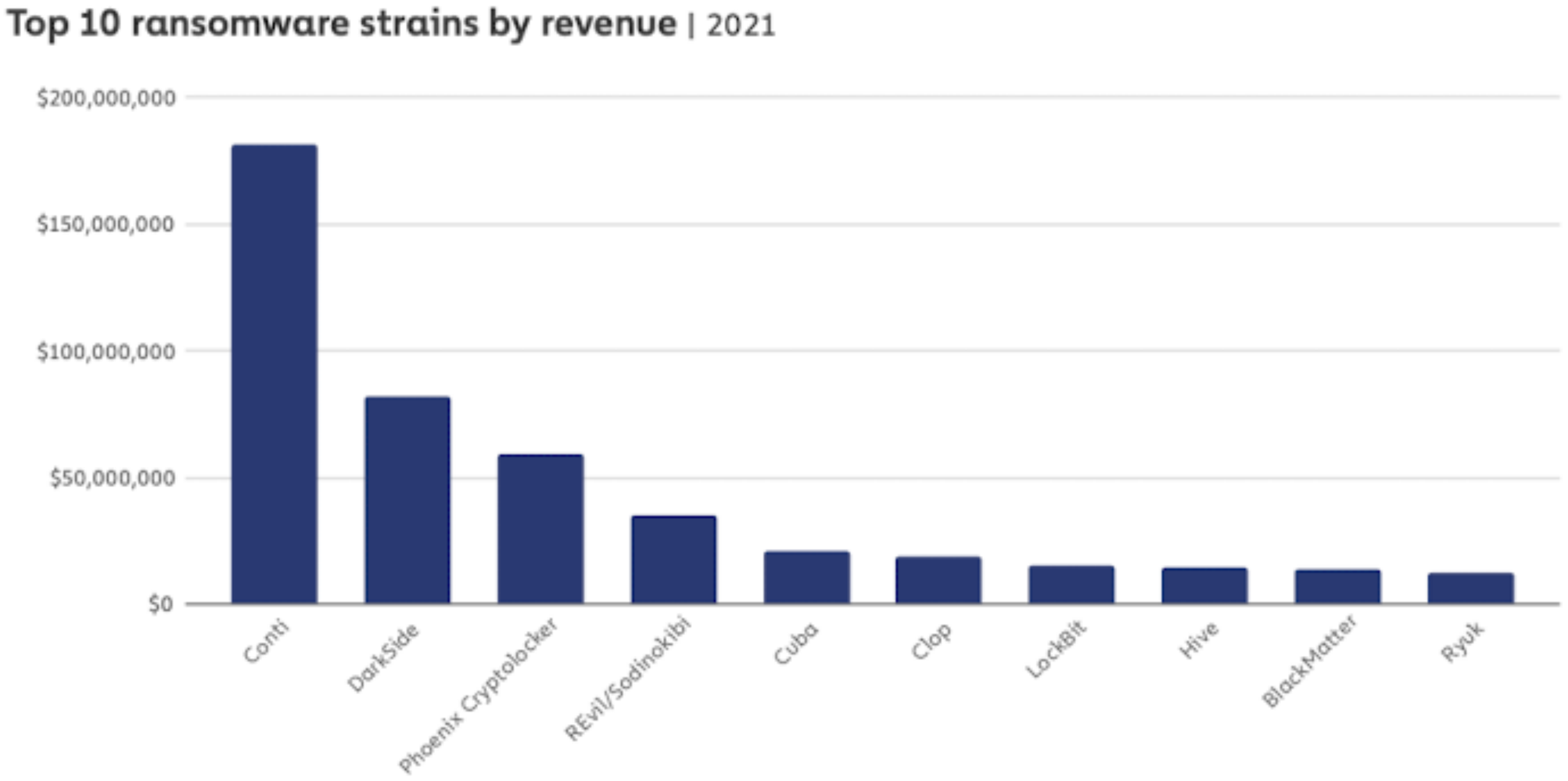
NFT Money Laundering

How can NFTs be used for money laundering?

WEB 3
LAW CENTER

Cryptocurrency and Crime

Ransomware



WEB 3
LAW CENTER

Cryptocurrency and Crime

Ransomware

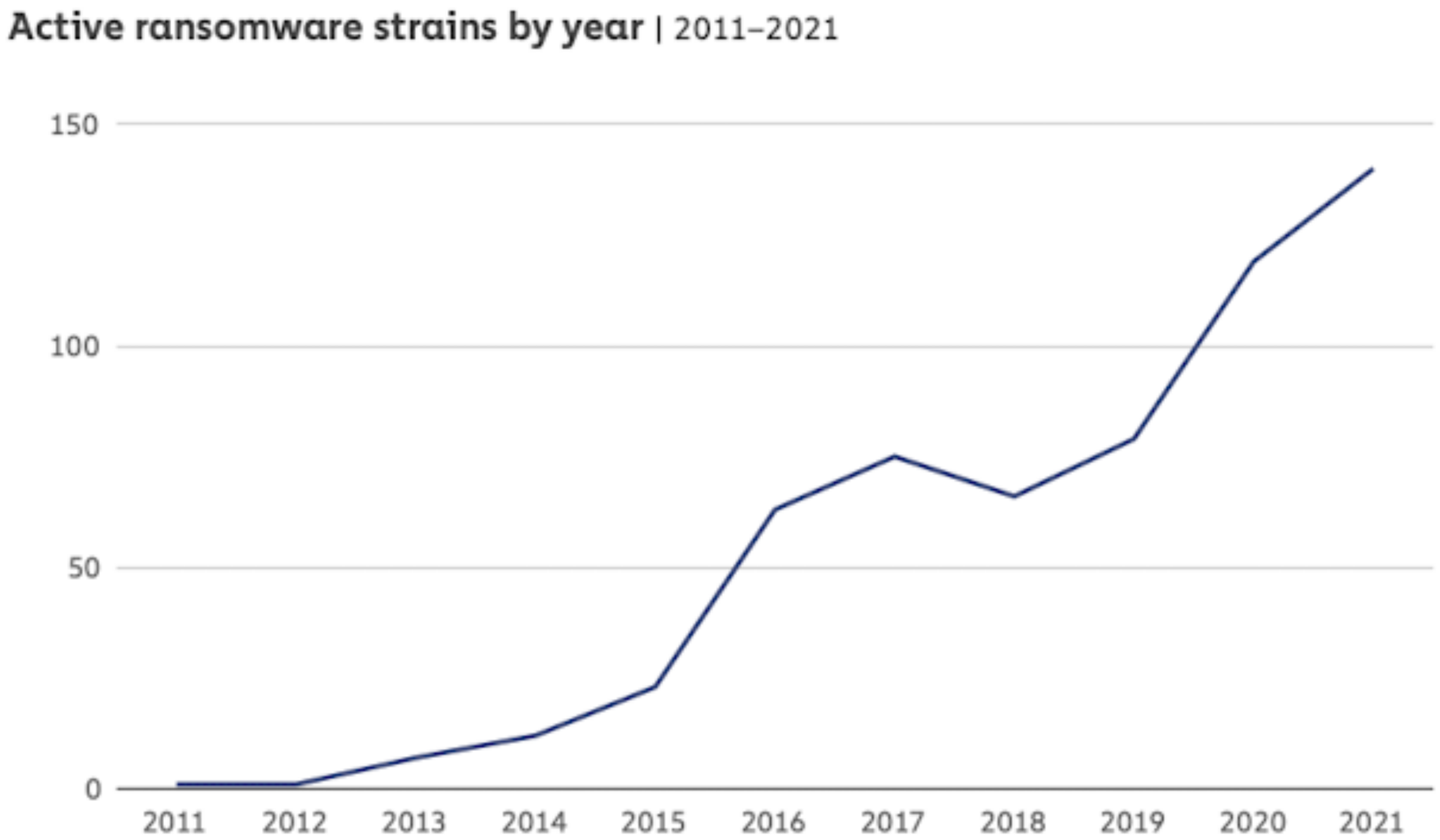
The Conti ransomware operates as a service wherein the extortion profit is shared between the RaaS owners and their affiliates. The affiliates are the entities or individuals who effectuate the computer intrusion and deploy the ransomware. Each affiliate uses its own intrusion method and the group negotiates the terms of the ransom demands with the victim.

Conti - Ransomware-as-a-Service

WEB 3
LAW CENTER

Cryptocurrency and Crime

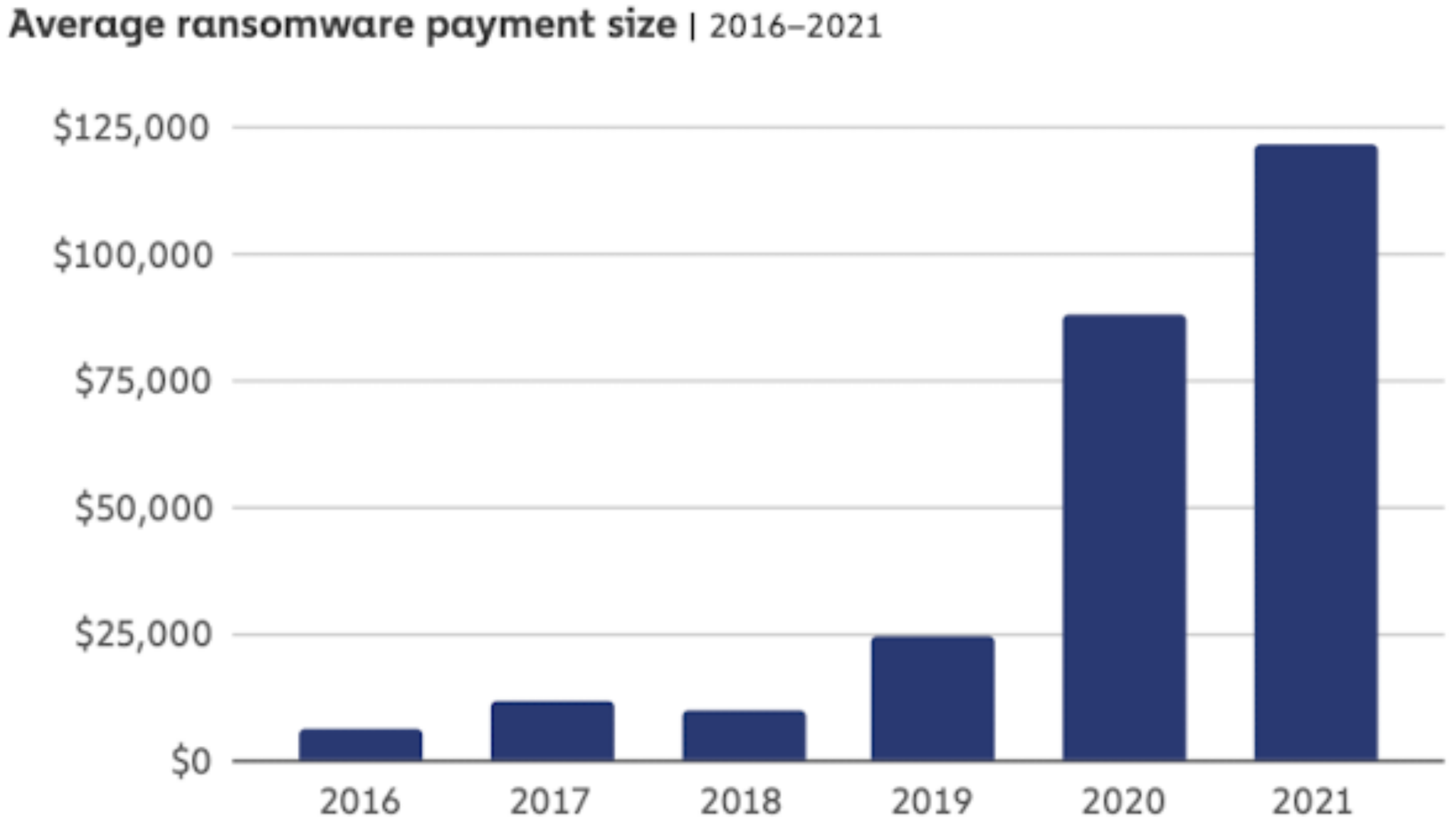
Ransomware



WEB 3
LAW CENTER

Cryptocurrency and Crime

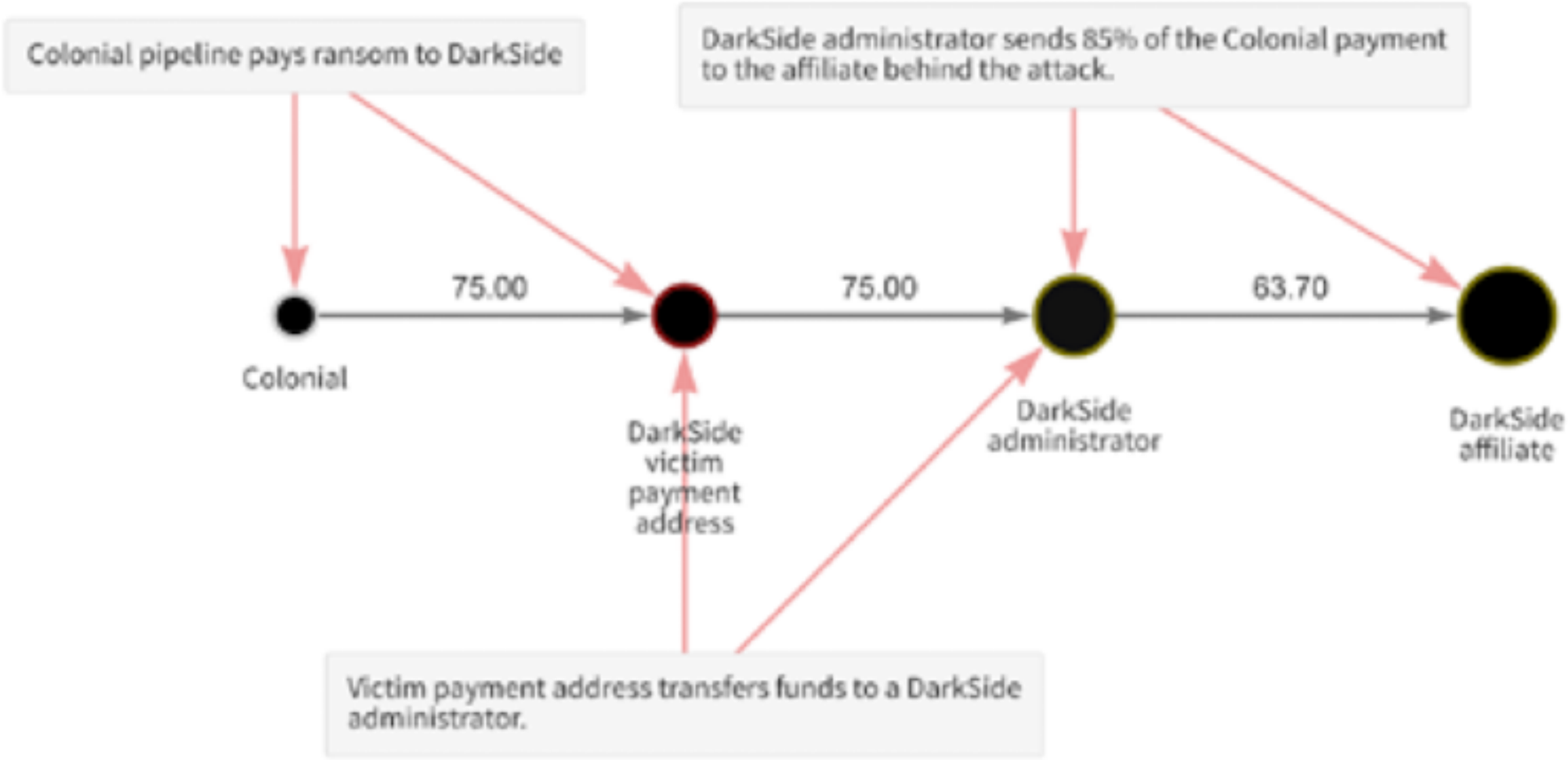
Ransomware



WEB 3
LAW CENTER

Cryptocurrency and Crime

Ransomware



WEB 3
LAW CENTER

Cryptocurrency and Crime

Ransomware

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Monday, June 7, 2021

Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside

WASHINGTON - The Department of Justice today announced that it has seized 63.7 bitcoins currently valued at approximately $2.3 million. These funds allegedly represent the proceeds of a May 8, ransom payment to individuals in a group known as DarkSide, which had targete
operation. The seizure warrant was authorized
Northern District of California.

"Following the money remains one of the mos
Monaco for the U.S. Department of Justice. "F
today's announcement demonstrates that the U
less profitable for criminal enterprises. We wi
these attacks. Today's announcements also demonstrate the value of early notification to law enforcement; we thank Colonial Pipeline for quickly notifying the FBI when they learned that they were targeted by DarkSide."

"There is no place beyond the reach of the FBI to conceal illicit funds that will prevent us from imposing risk and consequences upon malicious cyber actors," said FBI Deputy Director Paul Abbate. "We will continue to use all of our available resources and leverage our domestic and international partnerships to disrupt ransomware attacks and protect our private sector partners and the American public."

As alleged in the supporting affidavit, by reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim's ransom payment, had been transferred to a specific address, for which the FBI has the "private key," or the rough equivalent of a password needed to access assets accessible from the specific Bitcoin address. This bitcoin represents proceeds traceable to a computer intrusion and property involved in money laundering and may be seized pursuant to criminal and civil forfeiture statutes.

WEB 3
LAW CENTER

Cryptocurrency and Crime

Malware

Type	Description	Example
Info stealers	Collect saved credentials, files, autocomplete history, and cryptocurrency wallets from compromised computers.	Redline
Clippers	Can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace cryptocurrency addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets.	HackBoss
Cryptojackers	Makes unauthorized use of victim device's computing power to mine cryptocurrency.	Glupteba
Trojans	Virus that looks like a legitimate program but infiltrates victim's computer to disrupt operations, steal, or cause other types of harm.	Mekotio banking trojan

WEB 3
LAW CENTER

Cryptocurrency and Crime

Theft

Victim	Amount stolen (USD)	Service Type	Hack Type	Description
Poly Network	$613 million	DeFi platform	Code exploit	An attacker exploited cross-chain relay contracts to extract Poly Network funds from three different chains: Ethereum, BSC, and Polygon. The attacker ultimately returned the stolen funds. Read our complete case study.
BitMart	$200 million	Exchange	Security Breach	Attackers stole a private key that compromised two of BitMart's hot wallets.
BadgerDAO	$150 million	DeFi platform	Security Breach	Attackers used a compromised cloudflare API key to periodically inject malicious scripts into the Badger application. The scripts intercepted transactions and prompted users to allow a foreign address to operate on the ERC-20 tokens in their wallet. Once approved, the attacker siphoned funds from the user's wallets.
Undisclosed	$145 million	Private	Other — Embezzlement	Employee allegedly diverted funds to a personal account when the company attempted to transfer funds between financial accounts.

WEB 3
LAW CENTER

Cryptocurrency and Crime

Theft

Cream Finance	$130 million	DeFi platform	Flash Loan	First, attackers initiated a series of flash loans to mint ~$1.5M of crYUSD. Then, the attacker took advantage of Cream's PriceOracleProxy function to artificially inflate the value of its crYUSD to ~$3B. $2B of this was withdrawn in order to repay the attacker's outstanding flash loans, while the remaining $1B was used to drain all of Cream's assets available for lending ($130M).

WEB 3
LAW CENTER

Cryptocurrency and Crime

Scams

Investment Scams and Rug Pulls

AnubisDAO and the ANKH token
$60,000,000

WEB 3
LAW CENTER

Cryptocurrency and Crime

Scams

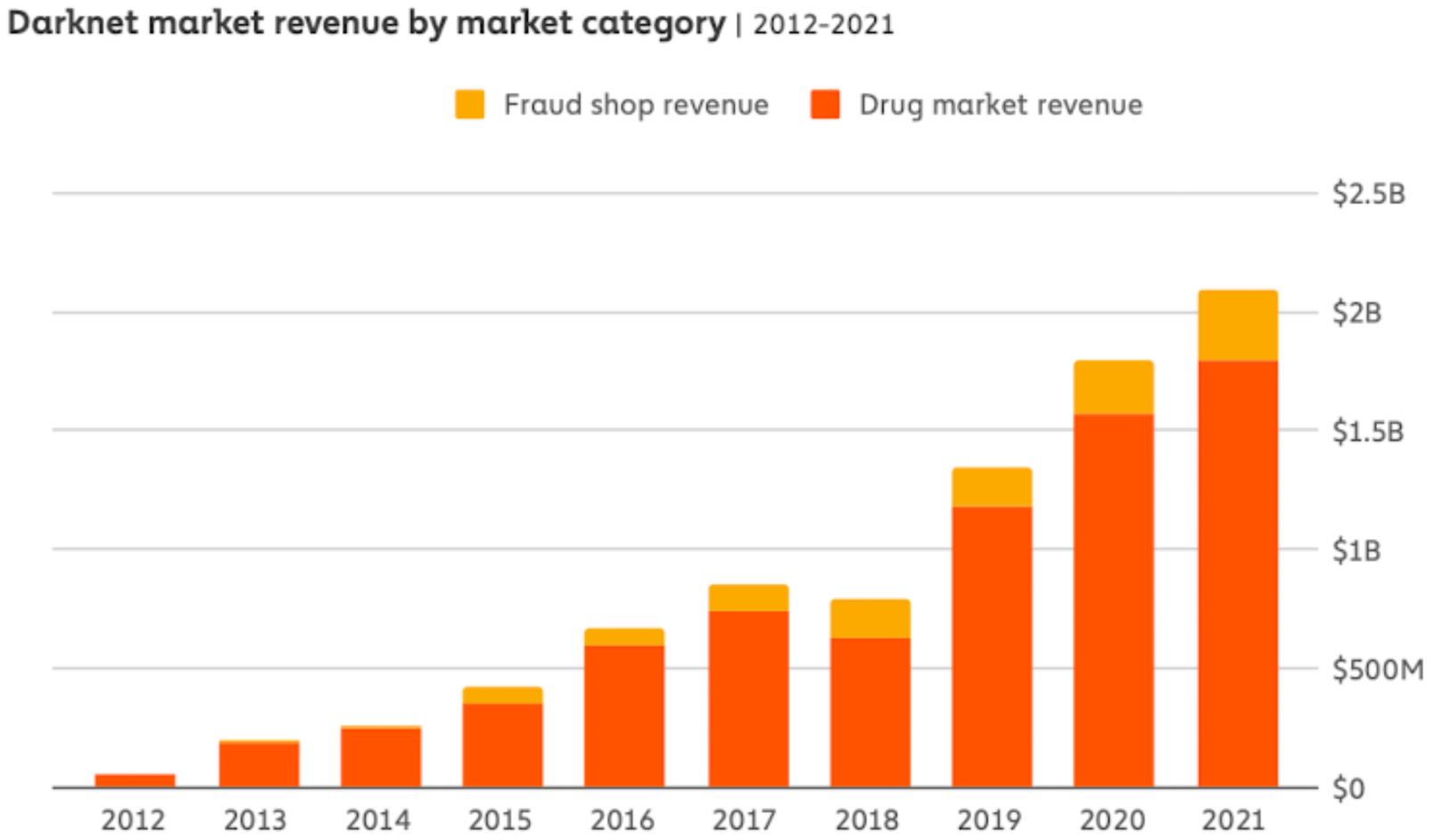
Investment Scams and Rug Pulls

Invest in only hard currency and provide 30% returns per month

WEB 3
LAW CENTER

Cryptocurrency and Crime

Darknet Markets



WEB 3
LAW CENTER

Quiz

https://www.medmalfirm.com/quiz/blockchain

WEB 3
LAW CENTER

Housekeeping

Assorted

Reminder that next week we will have a guest lecturer for both Monday and Wednesday's class.

WEB 3
LAW CENTER

Tech Note

Google Colab

Google Colab is an online terminal that allows the creation of Jupyter Notebooks running python code.

https://colab.research.google.com/drive/1G7XXYu4XZrrMlOiRB23cx7liI-WgGNdg?usp=sharing

WEB 3
LAW CENTER

News Note

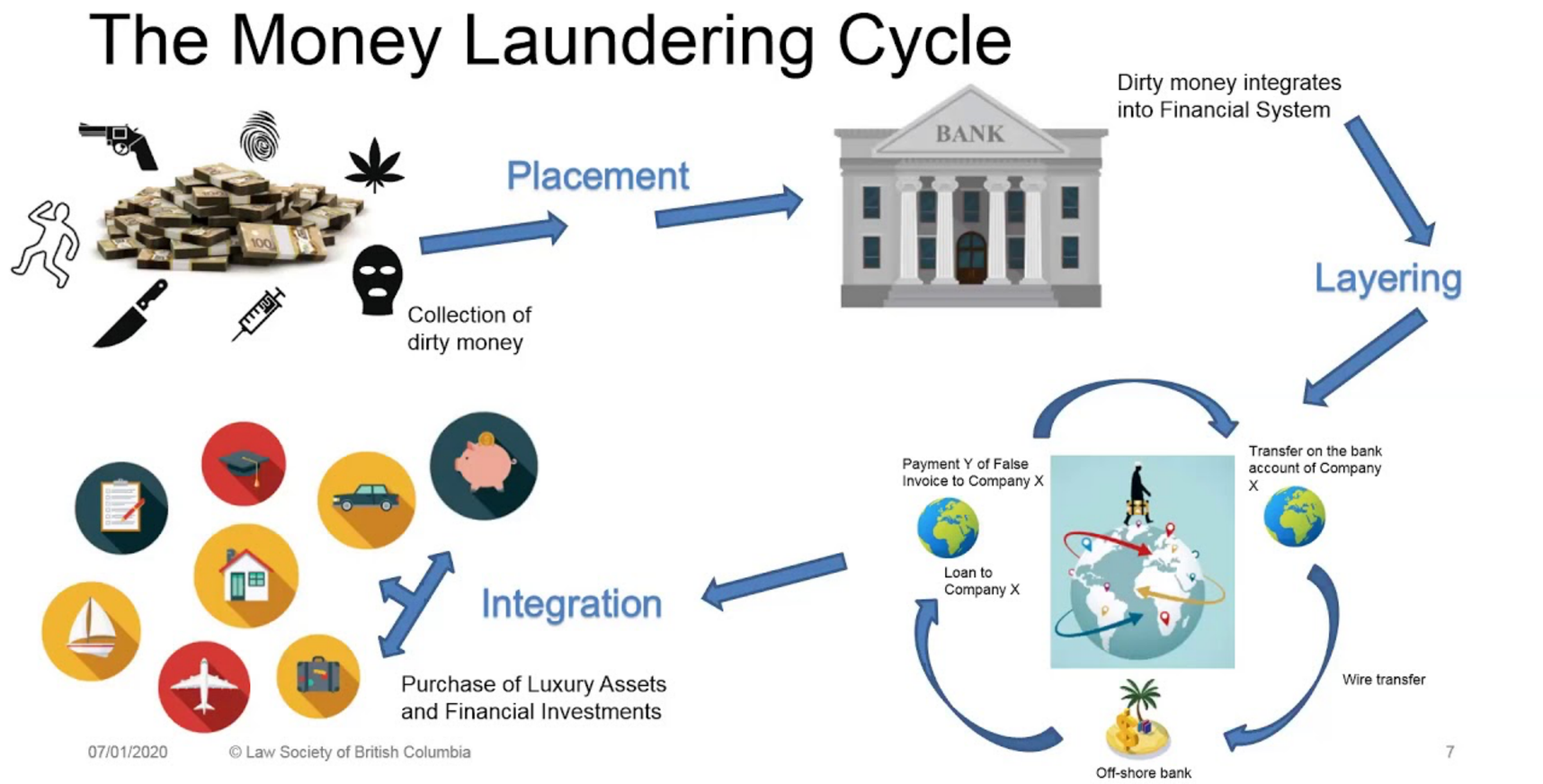
Starbucks to Offer NFT-Based Loyalty Program Using Polygon's Blockchain Technology

Polygon is a proof of stake chain that operates on top of the Ethereum network and offers reduced gas fees and transaction times.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

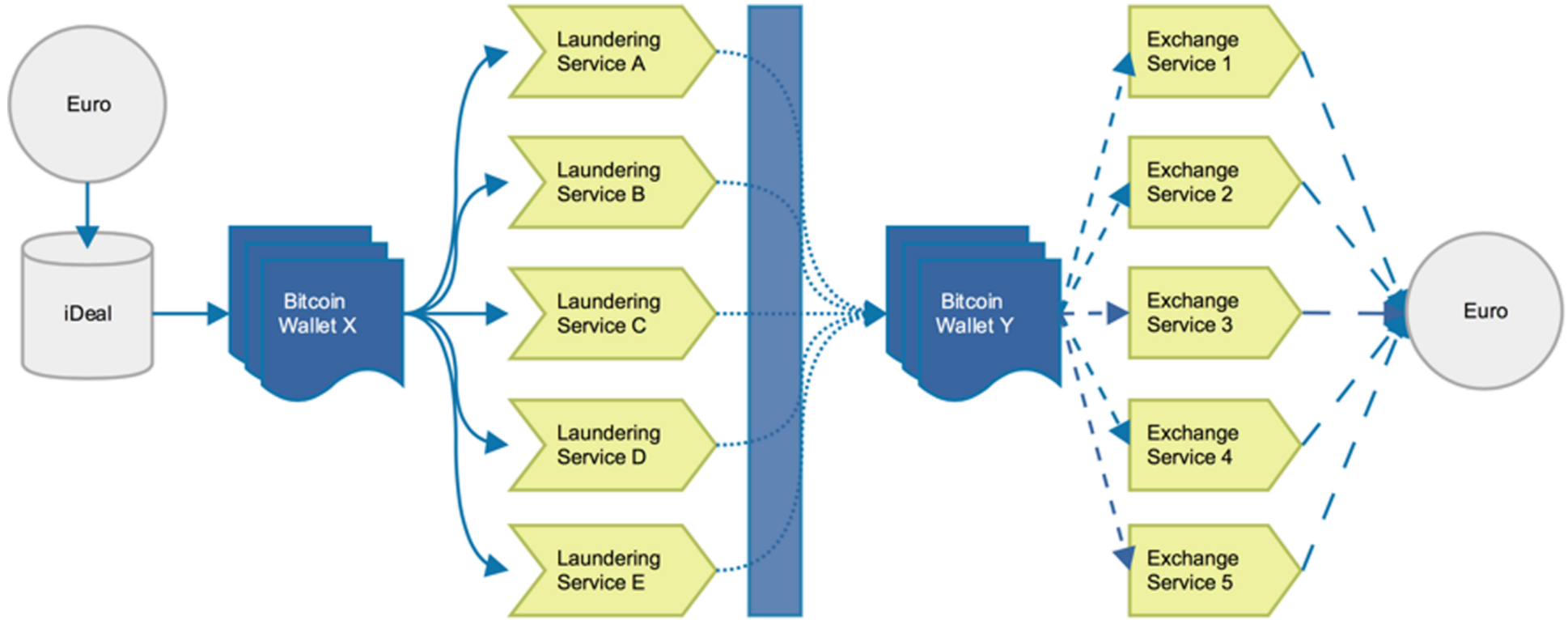
Cryptocurrency Concerns



WEB 3 LAW CENTER

Money Laundering, TF, and PF

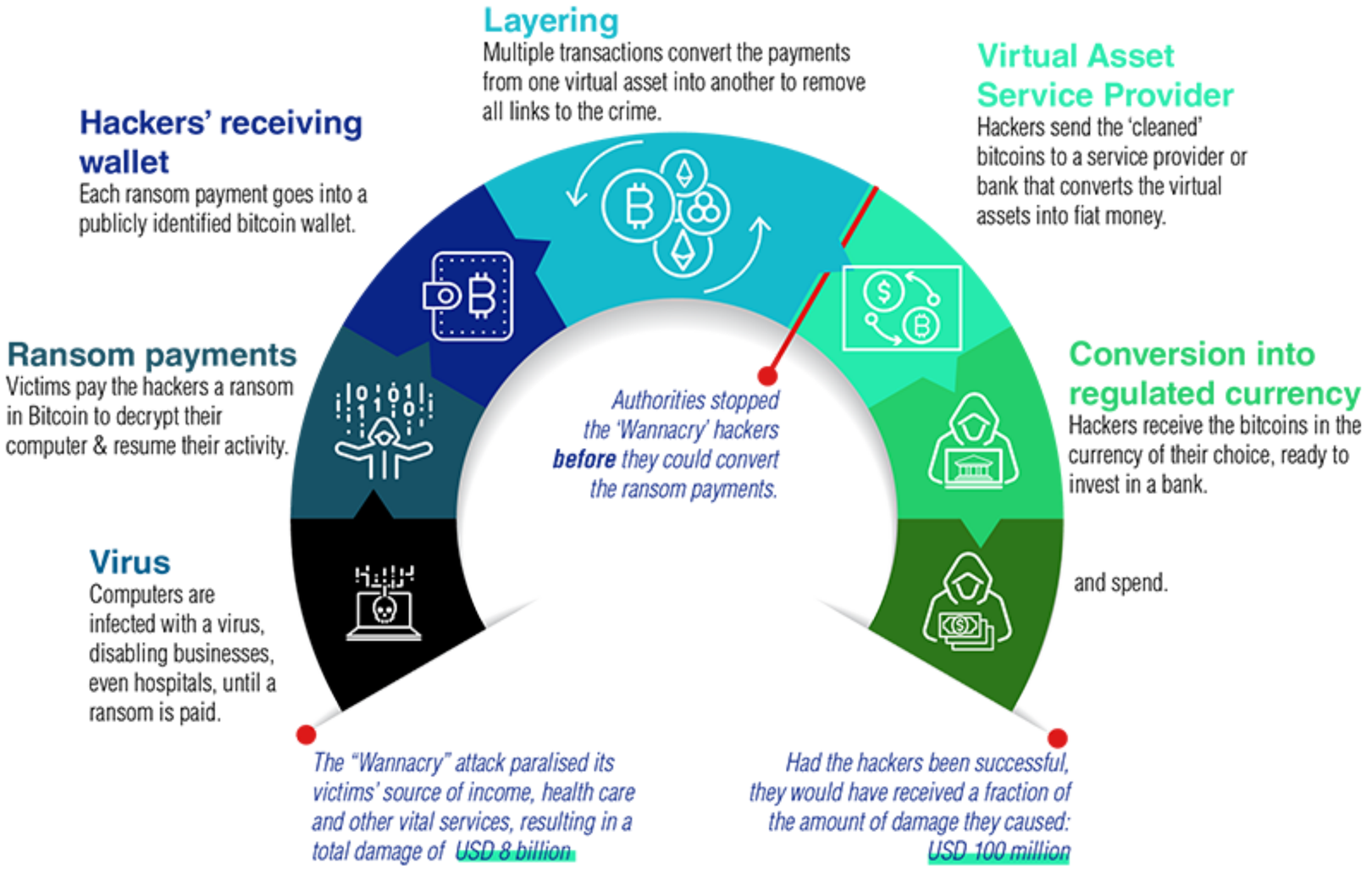
Cryptocurrency Concerns



WEB 3 LAW CENTER

Cryptocurrency as a Payment System

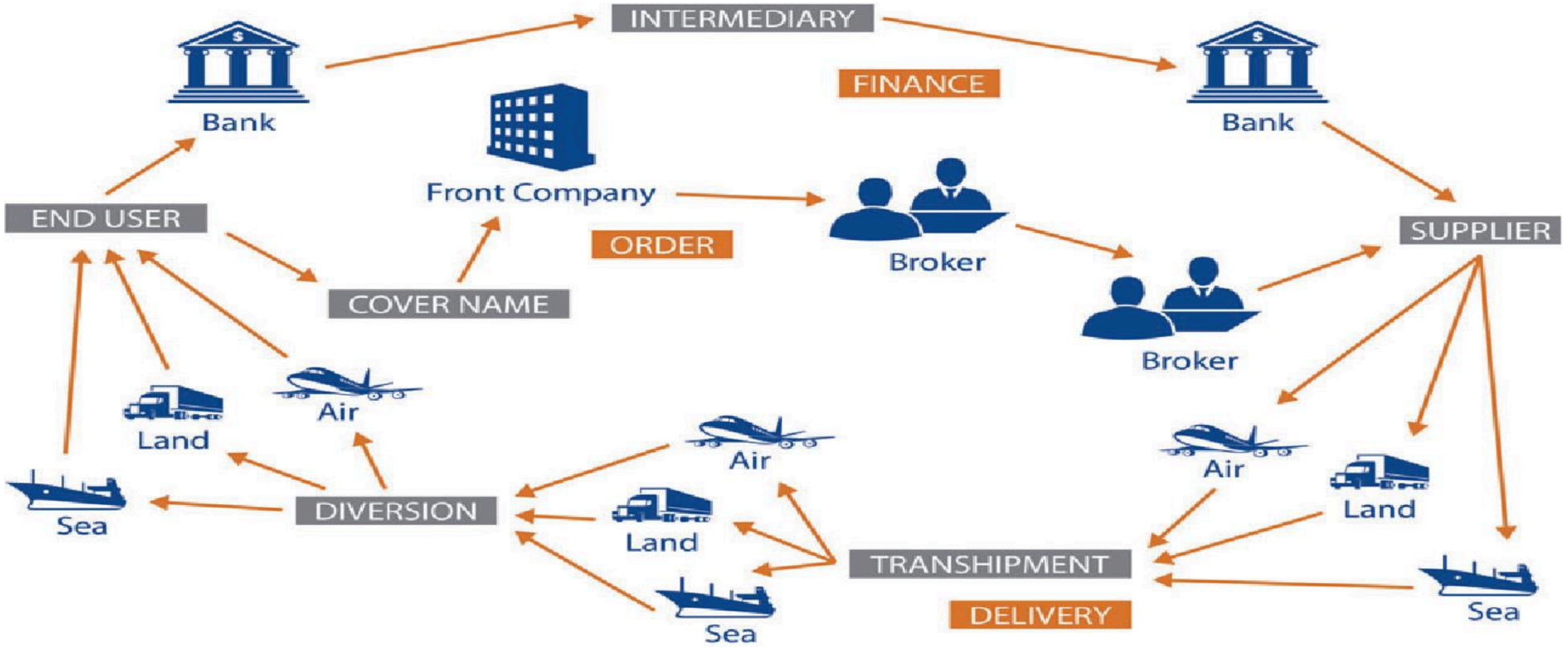
How hackers use cryptocurrency (according to FATF)



WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns



WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

Le Groupe d'action Financière (GAFI)
Financial Action Task Force
https://www.fatf-gafi.org

The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. The FATF has developed the FATF Recommendations, or FATF Standards, which ensure a co-ordinated global response to prevent organised crime, corruption and terrorism. They help authorities go after the money of criminals dealing in illegal drugs, human trafficking and other crimes. The FATF also works to stop funding for weapons of mass destruction.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

Placement — Layering — Integration

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations

WEB 3
LAW CENTER

Money Laundering, TF, and PF

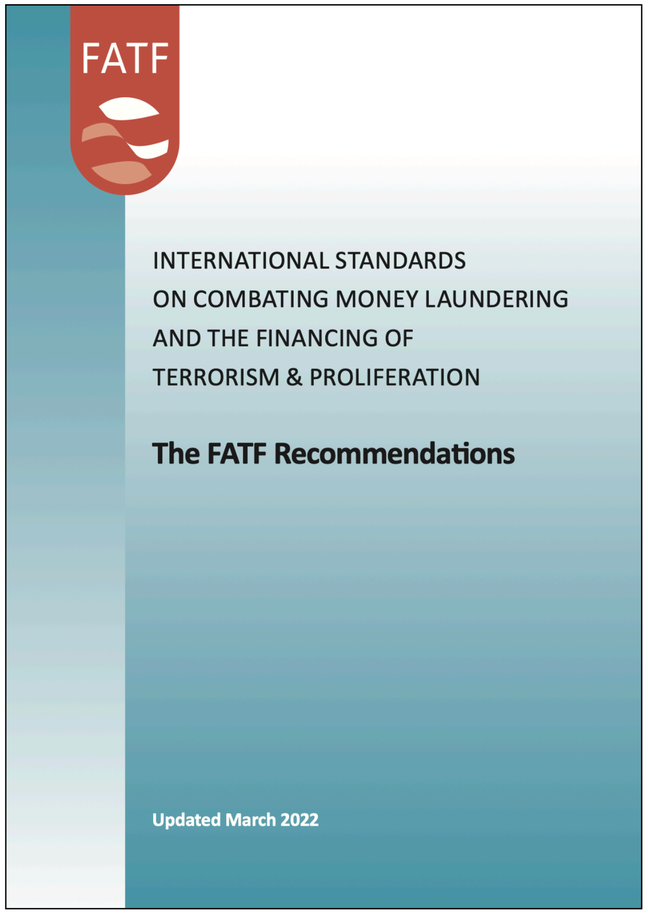
Cryptocurrency Concerns

Terrorism financing the financial of terrorist acts, terrorists, and terrorist organizations. A terrorist act includes any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns



The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats.

The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 1: A risk-based approach.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 2: National Cooperation and Coordination

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 6/7/35: Sanctions

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 10: Customer Due Diligence and Know Your Customer

Customers should be ranked based on how high risk or low risk they may be and monitored accordingly. Due diligence measures should be observed whenever a financial institution begins a new business relationship, when specific types of transactions take place, when there are doubts surrounding the customers' identity, and when there is suspicion of money laundering and/or terrorist financing.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 12: Politically Exposed Persons

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 15: New Technologies and Virtual Assets

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

Similar to other forms of payment (such as cash), there is a risk tolerance in the revised FATF Standards for a certain level of anonymous payments for virtual assets. The ML/TF risk for a specific so-called stablecoin, or virtual asset, will depend on how extensive anonymous peer-to-peer transactions with no intermediaries are within an arrangement and whether there are any other AML/CFT controls in place (e.g. transaction monitoring). Currently VASPs claim to offer an easier and more secure service to their users than peer-to-peer transactions. The comparatively greater friction and risk for customers of virtual assets through peer-to-peer transactions acts as a limiting factor on the number and value of peer-to-peer transactions. **If unmediated peer-to-peer transactions become easier and more secure, this could prompt a shift away from the use of VASPs. This could increase the number and value of payments not subject to AML/CFT controls and could present a material ML/TF vulnerability if mass-adopted.**

VIRTUAL ASSETS – FATF REPORT TO G20 ON SO-CALLED STABLECOINS

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 19: Higher Risk Countries

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 20: Reporting of Suspicious Transactions

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 22/23: Designated non-financial businesses and professions (casinos, real estate agents, dealers in precious metals and precious stones, trust and company service providers, notaries, lawyers, other independent legal professionals and accountants)

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 32: Cash Couriers

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Recommendation 36-40: International Cooperation

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

FATF Summary:

1. Risk-Based Assessment
2. Tracing and Due Diligence by all Financial and non-Financial businesses.
3. Reporting of Suspicious Behavior
4. International Cooperation (no shell banks, harboring, etc.)

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Cryptocurrency Concerns

Totally voluntary. Absolutely voluntary.

Failure to comply leads to the FATF Blacklist and the removal from all aspects of international trade.

But, really, voluntary.

WEB 3
LAW CENTER

Quiz

https://www.medmalfirm.com/quiz/blockchain

WEB 3
LAW CENTER

Housekeeping

Assorted

Reminder that next week we will have a guest lecturer for both Monday and Wednesday's class.

Feedback

WEB 3
LAW CENTER

Tech Note

What is a key-value pair?

As we learned, Python represents a list as [“AAPL”, “MSFT”, “META”]. A list has a set order from [0]:[n]. So, you can identify the third item in the list by referencing [2].

A dictionary is an unordered collection of key:value pairs. A dictionary is written like this:

```
myDictionary = {‘car’:’black’, ‘house’:’white’, ‘dog’:’brown’}
print(myDictionary[‘car’])
>>>black
```

WEB 3
LAW CENTER

News Note

Electrum Bitcoin Wallet Scam Suspect Is Arrested by Dutch Police

According to the police, the suspect had laundered tens of millions of euros (tens of millions of U.S. dollars) and had sought to cover his tracks using privacy coin monero (XMR) and decentralized exchange Bisq. He was identified through bitcoin (BTC) transactions.

In a bid to curb money laundering, the European Union recently passed new measures to make it harder to stay anonymous when using crypto. Jurisdictions such as the U.K. and France are also seeking to make it easier for police to seize crypto assets during investigations.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

US Compliance

Table 2. Technical compliance with re-ratings, February 2020

R 1	R 2	R 3	R 4	R 5	R 6	R 7	R 8	R 9	R 10
PC	C	LC	LC	C	LC	LC	LC	C	LC
R 11	R 12	R 13	R 14	R 15	R 16	R 17	R 18	R 19	R 20
LC	PC	LC	LC	LC	PC	LC	LC	LC	PC
R 21	R 22	R 23	R 24	R 25	R 26	R 27	R 28	R 29	R 30
C	NC	NC	NC	PC	LC	C	NC	C	C
R 31	R 32	R 33	R 34	R 35	R 36	R 37	R 38	R 39	R 40
LC	C	LC	LC	LC	LC	LC	LC	LC	C

WEB 3
LAW CENTER

Money Laundering, TF, and PF

US Compliance

Department of Treasury

FinCEN

Financial Crimes Enforcement Network

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

WEB 3 LAW CENTER

Money Laundering, TF, and PF

US Compliance

Department of Treasury

FinCEN

Financial Crimes Enforcement Network

FinCEN is becoming an international leader in the fight against financial crimes and the corresponding corruption of international economies. FinCEN supports the G-7 Financial Action Task Force (FATF), which came under the presidency of the United States for the seventh round (1995-96). In addition, FinCEN coordinates with financial intelligence units (FIUs) in scores of countries, including Britain, France, Belgium and Australia. FinCEN is also using its expertise to help establish FIUs worldwide.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

US Compliance

Department of Treasury

FinCEN

Financial Crimes Enforcement Network

31 U.S.C. 310

This statute establishes FinCEN as a bureau within the Treasury Department and describes FinCEN's duties and powers to include:

Maintaining a government-wide data access service with a range of financial transactions information

Analyzing and disseminating information in support of law enforcement investigatory professionals at the Federal, State, Local, and International levels

Determining emerging trends and methods in money laundering and other financial crimes

Serving as the Financial Intelligence Unit of the United States

Carrying out other delegated regulatory responsibilities

WEB 3 LAW CENTER

Money Laundering, TF, and PF

US Compliance

Department of Treasury

FinCEN

Financial Crimes Enforcement Network

By delegated US Treasury order, FinCEN is responsible for implementing, administering, and enforcing compliance with the Bank Secrecy Act, USA PATRIOT ACT, the AML Act, and the Corporate Transparency Act.

WEB 3 LAW CENTER

Money Laundering, TF, and PF

Bank Secrecy Act

Originally passed in 1970, the Bank Secrecy Act was intended to force the reporting of records that would have a high degree of usefulness in criminal tax proceedings.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Bank Secrecy Act

A Currency Transaction Report must be filed for cash transactions over $10,000.

Hypo: If a customer deposits $6000 in cash into his account at 9:30 a.m. and returns after lunch to make a $5000 cash loan payment, should a CTR be filed?

Answer: Yep.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Bank Secrecy Act

Suspicious Activity Reports must be filed for suspicious transactions of $2000 or more. The customer is not notified of the filing.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Bank Secrecy Act

Prohibits structuring of transactions to avoid the currency reporting requirement.

Money Laundering, TF, and PF

Bank Secrecy Act

FinCEN's Five Pillars of Compliance:

1. Designation of a Compliance Officer
2. Development of Internal Policies, Procedures, and Controls
3. Ongoing, Relevant Training of Employees
4. Independent Testing and Review
5. Customer Due Diligence Rule

WEB 3
LAW CENTER

Money Laundering, TF, and PF

Bank Secrecy Act

Customer Due Diligence (FATF Recommendation 10)

1. Identify and Verify Identity of Customers
2. Identify and Verify the Beneficial Owners of Accounts
3. Understand the Nature and Purpose of Customer Relationships to Develop Customer Risk Profiles
4. Conduct Ongoing Monitoring to Identify and Report Suspicious Activity and, On a Risk Basis, Maintain and Update Customer Information

WEB 3
LAW CENTER

Money Laundering, TF, and PF

FATF Recommendation 10

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

FinCEN Test

1. Are you a money service business (MSB)?
2. Have you registered as an MSB?
3. Do you have an effective, written “risk-based” AML program?
4. Have you complied with reporting and record keeping requirements?

WEB 3
LAW CENTER

Money Laundering, TF, and PF

FinCEN Test

FIN-2019-G001
The Financial Crimes Enforcement Network (FinCEN) is issuing this interpretive guidance to remind persons subject to the Bank Secrecy Act (BSA) how FinCEN regulations relating to money services businesses (MSBs) apply to certain business models1 involving money transmission denominated in value that substitutes for currency, specifically, convertible virtual currencies (CVCs).

WEB 3
LAW CENTER

Money Laundering, TF, and PF

FinCEN Enforcement

- Capital One: $390,000,000 for failing to implement and maintain an effective AML program.
- BitMEX: $100,000,000 for operating a virtual derivative trading platform without AML program.
- Helix and Coin Ninja: $60,000,000 for operating a mixer and operating an unlicensed money transmitting business. “advertised its services in the darkest spaces of the internet as a way for customers to anonymously pay for things like drugs, guns, and child pornography”
-

WEB 3
LAW CENTER

Money Laundering, TF, and PF

US Compliance

The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

WEB 3
LAW CENTER

Money Laundering, TF, and PF

OFAC Enforcement

- Tornado Cash Blacklisted in part because North Korean hacking collective that stole $620 million used it to store the money.
- OFAC “U.S. persons should be prepared to provide, at a minimum, all relevant information regarding these transactions with Tornado Cash, including the wallet addresses for the remitter and beneficiary, transaction hashes, the date and time of the transaction(s), as well as the amount(s) of virtual currency. OFAC would have a favorable licensing policy towards such applications, provided that the transaction did not involve other sanctionable conduct.”

WEB 3
LAW CENTER

Money Laundering, TF, and PF

OFAC Enforcement

OFAC said in its initial sanctions announcement that Lazarus Group, a North Korea-linked hacking entity, had sent millions of dollars worth of crypto through Tornado Cash, alleging that around 20% of the mixer's volume was tied to illicit activity.

"North Korea has increasingly relied on illicit activities – including cybercrime – to generate revenue for its weapons of mass destruction and ballistic missile programs," a Treasury spokesperson said via email.

"U.S. persons must comply with these sanctions. More broadly, we call on the cryptocurrency industry to do its part to prevent illicit activity – nation-state or otherwise – as that is what 'responsible innovation' requires," the spokesperson said. "This would include ensuring adequate cybersecurity measures, implementing know-your-customer measures, and complying with sanctions and anti-money laundering obligations. Treasury looks forward to continued dialogue with the virtual currency industry on these issues."

WEB 3
LAW CENTER