



Final Report

Empirical Study: The Role of Digital Assets and Evidence to Identify Human Trafficking

Traffick Free

PADM 5900

Intersection Consulting Team

May 16, 2023



Table of Contents

01	Introduction
03	Overview
04	Review of the Literature
06	Overview of Methodology
07	Cryptocurrency Serves as Payment Method for Ads
10	Blockchain Serves as Platform
13	NFT Serve as Product
16	Virtual Currency Serves as a Money Laundering Tool
21	Conclusions

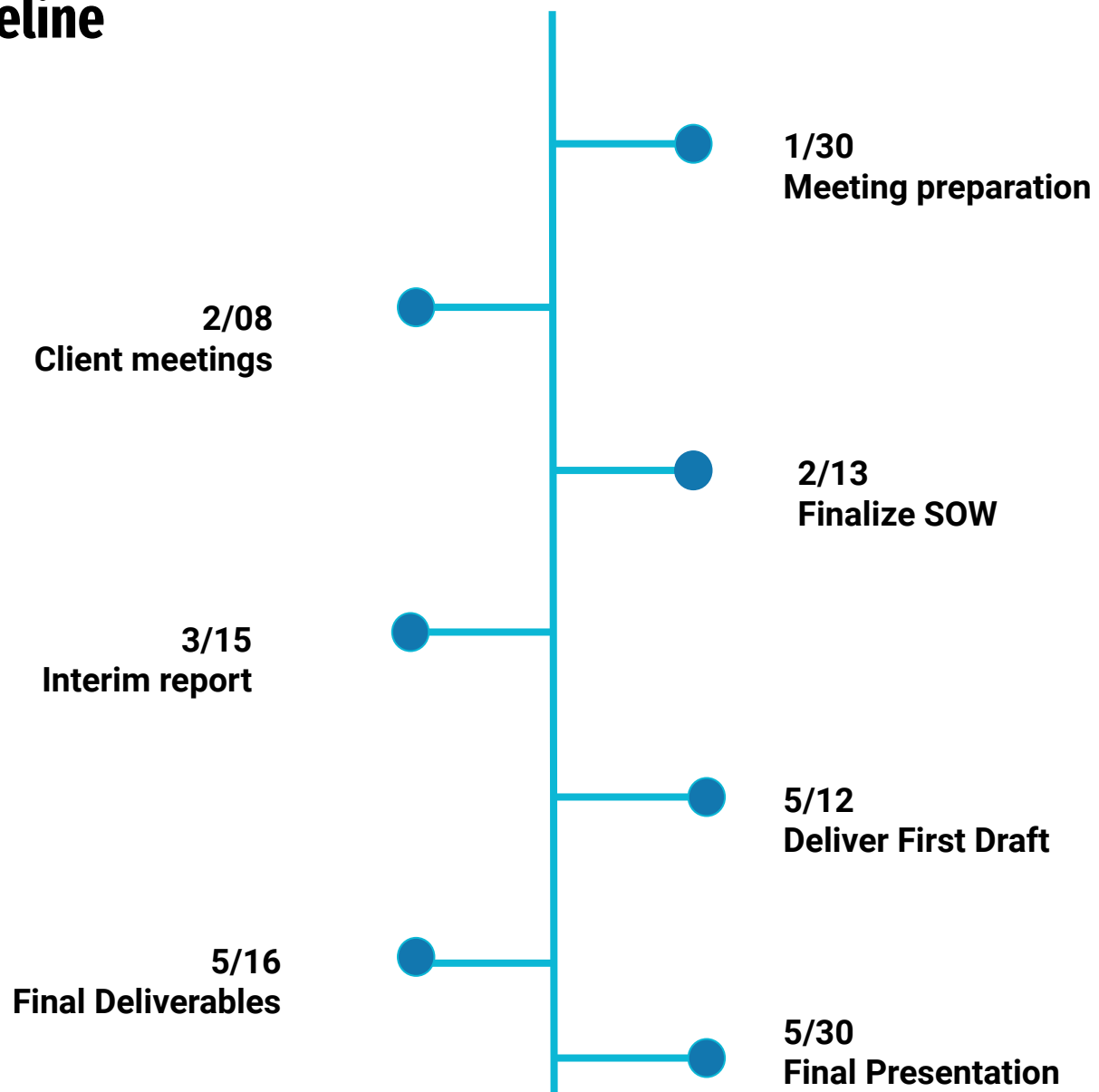


Introduction

Problem Statement

Cryptocurrency and digital assets have been intensely involved in transactions of human trafficking due to their anonymity¹. We aim to study how data detects human trafficking transactions and crypto's role. The study uses quantitative methods and case studies to address the problem.

Timeline



1. GAO, "VIRTUAL CURRENCIES: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking, 2.

Introduction

Mission and Value:

Intersection Consulting is made up of four Cornell first year MPA students Jingyun Yu, Puiman Shing, Rebecca Liu and Shirley Wang with diverse backgrounds in public policy, economics, finance and international development. As a consulting team, Intersection is committed to use their expertise and resources to add values to their clients. Our values of excellence and integrity guide us in all of our work, and we take pride in delivering exceptional results that exceed expectations. By partnering with non-profit organization Traffick Free, we hope to leverage our skills in strategy consulting and research to develop and implement practical solutions to the complex issue of human trafficking in finance.

Human trafficking refers to the illegal trade of human beings, often for the purpose of forced labor or sexual exploitation. It involves the exploitation of vulnerable individuals who are often lured or coerced into situations where they are exploited for the financial gain of traffickers. The involvement of digital currencies in human trafficking further complicates this already serious problem due to the pseudonymous nature of cryptocurrency-related transactions, many of which occur on the dark web. This makes tracking transactions associated with human trafficking a challenging task. Our objective is to gain insights into the qualitative and quantitative aspects of this issue by analyzing four case studies to identify the role and characteristics of digital assets in human trafficking.

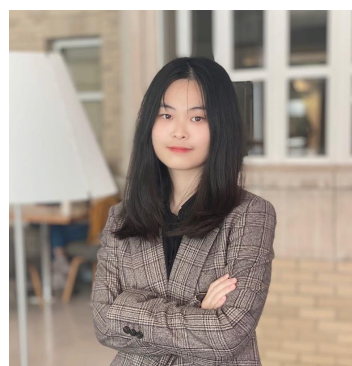
Jingyun Yu



Puiman Shing



Rebecca Liu



Shirley Wang

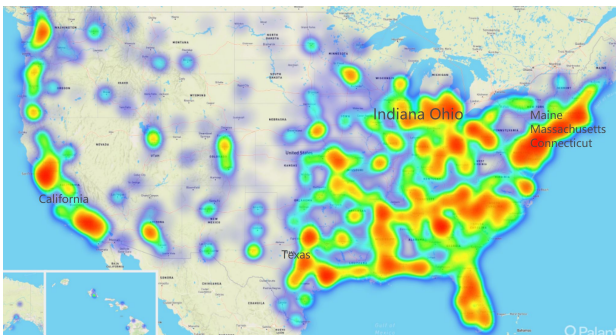


Overview

Human trafficking is a modern-day form of slavery that involves exploiting individuals through force, fraud, or coercion (National Human Trafficking Hotline ¹). It is a global phenomenon that affects millions of people every year. In the US alone, National Human Trafficking Hotline received a total of **51,073** substantive phone calls, text, Webchats, emails, or online tip reports nationwide (NHTH P1) ². Human trafficking can take many forms, including sex trafficking, forced labor, domestic servitude, and forced marriage. The top three types of trafficking reported in United States were **Escort Services** (10%), **Pornography** (8%), and **Illicit Massage, Health & Beauty** (8%) (Polaris P1) ³.

In recent years, human trafficking has become more tech-savvy. Digital assets are used in several ways to facilitate human trafficking. According to IRS (Internal Revenue Service, which is an U.S. federal agency that oversees the collection of taxes), digital asset broadly refers to any digital representation of value that is stored on a cryptographically secured distributed ledger, or any other similar technology ⁴. They are not real currency and common types include virtual currency, cryptocurrency and Non-fungible tokens (NFTs), which will be explained more in the later section.

Where are the cases? (2021)



Most cases in the United States happen in the eastern and coastal areas, such as Maine, Massachusetts, and Connecticut, and central places, like Indiana and Ohio ⁵.

Purpose: Forced Labor & Sexual Exploitation

2021 Form of Trafficking	2020		2021	
	# of Situations	% of Situations	# of Situations	% of Situations
Labor	1040	10%	1066	10%
Sex	7629	72%	7498	72%
Sex & Labor	339	3%	400	4%
Sex + Sex & Labor	7968	76%	7898	76%
Other/Not Specified ¹	1516	14%	1395	13%
Total Trafficking Situations	10524		10359	

The detection of tracking for sexual exploitation accounts for 72% of the total trafficking cases happening in 2021, indicating it is the primary purpose of human trafficking (Polaris P3) ³.

Recruitment Place

Detention Facility	4%
Group & Foster Home	2%
Internet	65%
School	5%
Other (Bus station, club...)	24%

The Internet remained the top reported recruitment location. So, it's the right time to pay more attention to **digital assets and online platforms**. (Polaris P16) ³

Recruitment Tactics

Reported Year	2020		2021	
	#	%	#	%
Abduction	282	6%	288	6%
Coercion (Threats, Blackmail, etc.)	190	4%	110	2%
False Promises/Fraud	312	6%	374	8%
Familial	1204	25%	1313	28%
Intimate Partner/Marriage Proposition	1111	23%	1143	24%
Job Offer/Advertisement	1713	35%	1462	31%
Posing as Benefactor	452	9%	414	9%
Smuggling-Related	109	2%	189	4%
Total Number of Victims with Known Recruitment Tactics	4863		4756	

The chart above shows the behaviors employed by potential recruiters and/or exploiters/traffickers to initially entice a likely victim into commercial sex or labor, or services. There are three effective tactics: through familial, intimate partner/ marriage proposition, or job offer/ advertisement. (Polaris P19) ³

Source:

1: National Human Trafficking Hotline, 2: National Human Trafficking Hotline Data Report, 2021 3: Polaris Analysis of 2021 Data, 2021 4: IRS 5: Polaris Myths, facts and Statistics

Review of the Literature

Human trafficking is a crime that trades and exploits a person for profit through illegal labor and commercial sex act using violence, deception, and coercion¹. According to the International Labour Organization report released in September 2022, an estimated 27.6 million people are victims of human trafficking around the globe, with \$150 billion in profits². The transaction of human trafficking can pay in cash, credit card, and virtual currencies such as bitcoin, which makes traffickers' transactions hard to trace. Consequently, it complicates the problem³ because cryptocurrency-related transactions are pseudonymous and mainly on the dark web⁴, a hidden internet site from public search. However, **knowing the roles and characteristics of the virtual currency associated with human trafficking in the dark economy is not impossible.**

The **money flow** related to human trafficking **has a specific pattern from reality to the online world**. Typically, trafficked victims are relocated from their initial holding location to where they will be exploited, sexually or in labor⁵. Next, human trafficking groups, especially sex trafficking ones, connect with buyers by advertising commercial sex online using digital assets like cryptocurrency⁶. After that, The financial transactions (proceeds) associated with human trafficking will be carried out either by perpetrators or money launderers in the human trafficking offense. **To convert virtual currencies to real currencies, traffickers can create accounts (digital wallets) on virtual currency, which later enables them to exchange virtual currency for fiat currency or other forms of currency⁷.** Nevertheless, the **illicit activities are heuristic and can be investigated** since most virtual currency transactions are **recorded on public blockchains⁸**. The information allows transaction investigators to monitor the transactions patterns like volume and purchase characteristics and create databases of transactions to identify payments linked to particular virtual currency wallets by using data mining and machine-learning algorithms⁹.

1. The meaning of human trafficking is defined by United Nations Office on Drugs and Crime. More information can see in [Global Report on Trafficking in Persons](#).

2. The number comes from [International Labor Organization's report](#) in 2022.

3. Team Praescient, [Inside a Bitcoin Bust: Tracing Money Laundering Practices Along a Cryptocurrency Network](#) (2022).

4. The dark web is a section of the World Wide Web that can only be accessed with specialized software, allowing users and website administrators to remain anonymous or untraceable.

5. Caltagirone, S. . [The human trafficking kill chain - global emancipation network](#). GLOBAL EMANCIPATION NETWORK. p.12 & p. 17

6. Financial Crimes Enforcement Network Advisory, [Identifying and Reporting Human Trafficking and Related Activity \(2020\)](#). p.5.

7. See p.1 of the report in footnote 6.

8. Yoichi Tsuchiya & Naoki Hiramoto, Dark web in the dark: Investigating when transactions take place on cryptomarkets. Forensic Science International: Digital Investigation(2021), p.1.

9. Government Accountability Office, [VIRTUAL CURRENCIES: Additional Information Could Help Improve Federal Agency Efforts to Counter Human and Drug Trafficking \(2021\)](#), p.2 & p.40.

Review of the Literature (Cont'd)

For example, with the public-listed bitcoin address information together with advanced analytical tools, the Internal Revenue Service Criminal Investigation (IRS-CI) successfully identified the administrator of the largest child sexual exploitation website, Welcome To Video, and eventually traced the physical location of the website server in South Korea¹⁰. Even more, the study work from Portnoff, Huang et al. concluded that obtaining explicit personally identifying information from digital wallets is possible by utilizing the automated clustering technique to match repetitive online advertisements with bitcoin transactions.

The ever-strict **virtual currency regulations** established a legal framework for public authorities and investors **to navigate and operate**. Studies have shown that the regulations can achieve the objectives of **a) monitoring the velocity of money, b) preventing illicit businesses and money laundering, and c) creating a new source of government revenue from tax**¹¹. For example, the Anti-Money Laundering Directive (ALMD) proposed in European Commission extends its scope to virtual currency, requiring the trading platforms to comply with customers' due diligence and the responsibility to identify, prevent, and report the transactions. On the one hand, the legal framework protects the users' rights as customers, ensuring the reliability of sustainability claims in the areas of human rights. On the other hand, the established legal system enables cryptocurrency trading to become easier to identify and more transparent in the event of illegal activities. For instance, individuals participating in illicit online actions often create accounts on digital currency exchanges without providing legitimate Know-Your-Customer (KYC) documents to hide their identity.

Based on this, law enforcement authorities dismantled DarkScandle, a website distributing sexually explicit materials, by connecting users from both websites with accounts that were registered on these exchanges. However, it does not indicate that accounts with validated and complete KYC information do not have the risk of exposure to illicit sex services¹².



10. More information can be found on The United States Department of Justice [website](#).

11. Ahmad Chokor & Elise Alfieri, [Long and short-term impacts of regulation in the cryptocurrency market](#) (2021).

12. The International Centre for Missing & Exploited Children and Standard Chartered, [Cryptocurrency and the Trade of Online Child Sexual Abuse Material](#) (2021), p.14.

Overview of Methodology

What & Why Case Study?

A **case study** is a research methodology that produces a thorough, multifaceted understanding of a complex problem in its actual setting. We adopt case studies because they can best meet our clients' needs, which provide the specific process of how and where cryptocurrency trades regarding human trafficking.

**CASE
STUDY**



In this report, we present **4 cases** to illustrate the usage of cryptocurrency in different contexts. The 4 cases focus on “Cryptocurrency Serves as a Payment Method”, “Blockchain Serves as a Payment Platform”, “NFT Serves as Product”, Virtual Currency Serves as a Money Laundering Tool”. Bases on the cases, we conclude some most common websites, platforms and approaches that facilitate human trafficking activities.

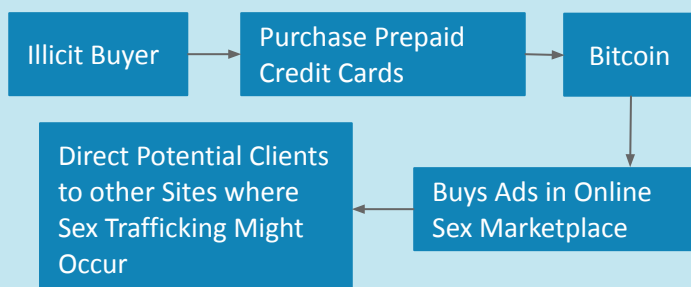
The Cases We Use

Cryptocurrency Serve as a Payment Method for Ads

Currency: payment method for ads

Cryptocurrency can be used as a method of payment to the trafficker to facilitate human trafficking. It can also be used as a way of dispersion of profits to all involved in trafficking the individual .

According to the FinCEN advisory ¹, trafficking groups purchase advertisements as a means of reaching out to potential buyers. The following flow chart illustrates the process.



Prepaid Credit Cards: prepaid cards, which allow for **anonymous acquisition with cash or via darknet websites**. These prepaid cards are used to register on escort websites and to buy sexual services, flights, disposable phones, and hotel accommodations.



Case Study

In 2016 ², Homeland Security Investigations responded to a call about a woman being held at an El Paso motel. They found two victims and arrested William "Tae" Harris. An investigation revealed that the victims were forced into prostitution and threatened with violence. Harris' phone contained bitcoin transaction data, which led to the discovery of their use of prepaid credit cards to buy bitcoin on **Paxful**, then used to purchase prostitution ads on **Backpage.com**.

Founded in 2015, **Paxful** ³ is a global peer-to-peer (P2P) cryptocurrency marketplace that enables users to buy, sell, and trade Bitcoin and other cryptocurrencies easily and securely. Paxful is registered as a Money Services Business (MSB) with FinCEN. Paxful has also obtained the necessary licenses and registrations in the jurisdictions where they are required to operate as a money transmitter.

Backpage ⁴ was a classified advertising site that operated from 2004 to 2018. It featured a controversial "adult" section for escort services, adult entertainment, and related services. Backpage faced legal challenges and controversy over allegations of facilitating prostitution and human trafficking, ultimately leading to its shutdown in 2018.

Source:

1: [The Payment Transaction of Sex Trafficking](#)

2: [Case Study](#)

3: [Paxful](#)

4: [Backpage](#)

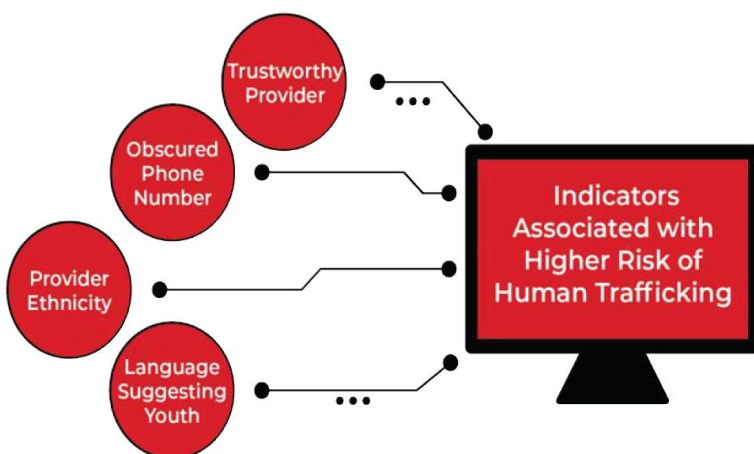
Cryptocurrency Serve as a Payment Method for Ads

Online Escort Ads Facilitate Human Trafficking

The case in El Paso, Texas, is just one example of how online escort ads and sex marketplaces can facilitate human trafficking. This issue has been a longstanding concern. In a 2018 report¹, the National Center for Missing and Exploited Children analyzed over 10,000 escort ads and found that nearly 75% of them were suspected of involving trafficking. Similarly, a study by the Urban Institute² found that ads on Backpage.com (which has since been shut down) were significantly more likely to be associated with trafficking than other online venues.

So, can we identify ads that are more likely to be associated with a trafficking case? The answer is YES. The Justice Research and Statistics Association and the Human Trafficking Intelligence Project³ studied on indicators of sex trafficking in online escort ads. By comparing ads belonging to trafficking cases with ads that did not, the study presented information on indicators of trafficking.

Indicators Associated with a HIGHER RISK of Trafficking



1. **Trustworthy Provider Language:** Providers in trafficking cases are more likely to use language that assures clients of their trustworthiness, such as "100% professional" and "discreet". Ads that contain these languages are more than four times as likely to be associated with trafficking cases.

2. **Obscured Phone Number:** Traffickers may use phone numbers that employ obfuscation techniques, such as **emojis between numerals**, **spelling out numbers**, or **extra spaces**, to avoid being detected by law enforcement and technology platforms.

3. **Provider Ethnicity:** Traffickers may provide explicit **choice of ethnicity or race** in their ads, to meet the desires of illicit buyers. Ads that describe the ethnicity of the victims are more than five times as likely to be linked with human trafficking cases.

4. **Language Suggesting Youth(use with caution):** Language communicating that **the provider is young** can be a coded message to sex buyers that **the provider is under 18**.

Source:

1. 2018 NCMEC Annual Report

2. Urban Institute. Findings from an Evaluation of the Enhanced Collaborative Model Task Forces to Combat Human Trafficking

3. Justice Research & Statistics Association. Indicators of Sex Trafficking in Online Escort Ads

Cryptocurrency Serve as a Payment Method for Ads

The study's insights can be helpful in improving the accuracy and efficiency for identifying victims of trafficking. However, Sex trafficking survivors consulted for the study emphasized that the presence of **indicators in escort ads should not be solely relied upon to draw definitive conclusions about sex trafficking**. Rather, escort ads should be used to narrow the focus of investigations, and not as a substitute for a thorough inquiry.

Online sex marketplaces are often where illicit buyers purchase these ads. The question remains, what can be done about escort advertisement websites? Backpage was shut down, but how? Can all escort advertisement websites be shut down? These are important considerations that need to be explored further.

How was Backpage shut down?

In April 2018, Backpage was shut down by the U.S. Department of Justice. It was a significant victory in the fight against human trafficking and sent a strong message to other websites that may be involved in similar activities. The case against Backpage was brought under the federal law known as **the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA)** and **the Stop Enabling Sex Traffickers Act (SESTA)**, which aimed to hold website owners and operators accountable for knowingly facilitating sex trafficking through their platforms. Federal agencies used an older law, **the Travel Act**, to go after Backpage. This 1961 law criminalizes traveling or using "the mail or any facility in interstate or foreign commerce" with the intent to "further any unlawful activity."

Can all escort ads websites be shut down?

Eight years ago, Craigslist was the primary platform for escort advertisements until it was shut down. Similarly, Backpage faced a similar fate, and despite the emergence of hundreds of similar websites, it seems impossible to completely eradicate them. These websites host legal sex-work ads that are protected under **the First Amendment**, as argued by former Backpage executives Larkin. Moreover, a shared concern among advocates is that **the crackdown on such websites will force sex workers to operate under more dangerous conditions**, as these platforms provide a reliable way for them to connect with potential clients. As such, it is essential to consider the potential implications of these takedowns and ensure that sex workers' rights and safety are protected.

Takeaways

Cryptocurrency has increasingly become a preferred payment method for illicit ads, including those used by traffickers to connect with potential buyers. Despite efforts to eliminate these ads, it is challenging to take down all websites that host them due to legal protections and their significance for sex workers. To combat sex trafficking, institutions can utilize indicators discussed to identify potential trafficking activities within these ads. However, given the constantly evolving nature of these activities, institutions must continually develop new tools to identify and prevent trafficking through ads. As part of these efforts, it is essential to balance the need to protect the rights and safety of sex workers while also working to eliminate trafficking activities.

What is Blockchain?

Blockchain is defined as a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. There are **three key elements** for blockchain:



Distributed ledger technology

Every network participant has their own ledger which has no centralized administration.



Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger.



Smart contracts

A set of rules which is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more¹.

What is Spankpay?



SpankPay is a **payment processing platform** that allows **adult content** creators and merchants to accept cryptocurrency payments, including SpankChain (SPANK), Bitcoin (BTC) and Ethereum (ETH). Spankpay is a payment platform developed by the **SpankChain** company².



The graph above established the relationship among several features within SpankChain Company. **SpankChain** is the company which is an entirely new **financial ecosystem** on the blockchain who aim to provide services for adult industry. Spankpay is the payment platform that specifically for adult industry which is developed by SpankChain. **SPANK Token** is the **virtual currency** developed by SpankChain to trade in the ecosystem³.



The graph above established **how SpankPay works as a payment platform**. First, users create their accounts on Spankpay and connect their bank accounts to Spankpay. Users have different input currency like Bitcoin and Ethereum which can be converted into fiat currency through Spankpay. The types of fiat currency can be converted for Spanky include Dollars, Pounds and Euros. **How does SpankPay make the conversion?** Spankpay partner with **Wyre** which is a regulated Money Service Business (MSB), which means it is a financial services provider licensed to transmit and convert money⁴.

1. IBM, What is blockchain technology?, 1, <https://www.ibm.com/topics/blockchain>
2. Spankchain, What is Spankpay?, 1, <https://spankchain.freshdesk.com/support/solutions/articles/69000232094-what-is-spankpay->
3. Spankchain, Token, 1, <https://spankchain.com/token/>
4. Terraforte, What is Wyre?, 2, <https://wyre-support.zendesk.com/hc/en-us/articles/360055622634-What-is-Wyre->

Blockchain Serve as Platform

How does Spankpay Work?

1. **Sign up for an Spankpay account**
 - a. You only need a email address to sign up the Spankpay account
2. **On boarding**
 - a. Step 1: Complete Your Profile
 - b. Step 2: Tax Information
 - c. Step 3: Select you Holding Currency
 - d. Step 4: Setup Banking

Information entered here will allow the partner, **Wyre**, to process withdrawals to your bank account¹.



Wyre: Company Behind Spankpay

What is Wyre?

Wyre is an **exchange** that offers **crypto to fiat** and compliance solutions via API and dashboard. It is a regulated **Money Service Business (MSB)** founded in 2013. Wyre is the leading **infrastructure provider** in crypto, bridging the gap between traditional payment processing and digital assets. In conclusion, Wyre is the **technology infrastructure provider for Spankpay** who collect the most information from the users².

Insights:



It is possible for **pornography websites** with a potential for human trafficking to collaborate with **third-party exchange companies**. This collaboration allows these websites to facilitate financial transactions and process payments for their services. In this case, Wyre is the third-party exchange company who provides services to Spankpay. We highly **recommend** investigator to pay attention with third-party service providers behind possible website and platform to gain useful information.

Information Wyre Collected

In order to complete the conversion, there are several information that Wyre need to collect.

1. **Account Information**
 - a. Telephone number, machine or mobile device ID.
2. **Identification Information**
 - a. Your name, street address, email address, date of birth, and SSN
3. **Device Information**
 - a. **From your mobile device** such as device type, machine or mobile device identification number, geo-location, time zone, language setting, browser type, and IP address
 - b. **From third parties** for purposes of transaction processing, identity verification, fraud detection or prevention and other similar purposes.
 - c. **For fraud prevention purposes**, we also may link your machine ID with the machines of others who use your same payment cards.
4. **Financial Information**
 - a. Bank account and routing numbers and credit cards linked to your Wyre account.
5. **Know Your Customer (KYC) Information**
 - a. Information collected through a W-9 and other Identification Information³.



Takeaways

Wyre possesses the majority of the **Know Your Customer (KYC) data**; however, they do not bear the legal obligation to to retain such information. The presence of significant risks arises for Spankpay due to the inability to acquire crucial data and the consequent lack of capacity to effectively track instances of human trafficking.

Recommendation: The **government** should conduct thorough **investigations** into third-party entities that provide cryptocurrency services to pornography websites, urging them to **strengthen** their Know Your Customer (KYC) protocols. Additionally, it is advised to initiate tracking efforts starting from individuals who have already been **apprehended**.



1. Spankchain, Solution Home, <https://spankchain.freshdesk.com/support/solutions/69000142636>
 2. Terraforce, What is Wyre?, 2, <https://wyre-support.zendesk.com/hc/en-us/articles/360055622634-What-is-Wyre>.
 3. Wyre, Private Policy, 4, <https://www.sendwyre.com/legal/privacy-policy>

NFT Serve as Product

What is NFT?

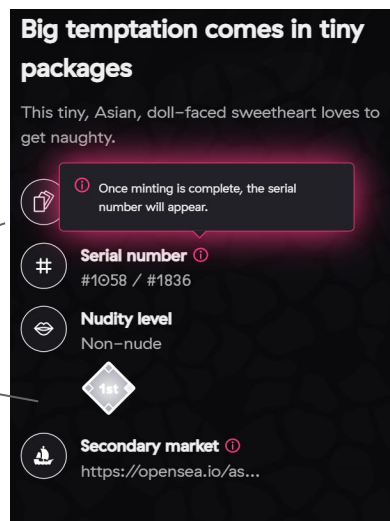
NFT stands for Non-Fungible Token, a type of digital asset representing ownership of a **unique** item. Unlike cryptocurrencies or fiat currency, which are interchangeable, NFTs are one-of-a-kind with unique serial numbers and properties that make them distinguishable from one another. NFTs are created on a **blockchain**, using smart contracts to verify ownership, transfer ownership, and track the history of the asset.

Case Study: Pop Shots NFTs

Pop Shots: are NFTs sold in a pack of 4. Each NFT features a sex worker and is one-of-a-kind with a different serial number. Users can use ETH or BTC in their Spank Pay Wallet to purchase newly released Pop Shots on pornographic websites or buy from owners from the Secondary market.

Each contains an unique serial number

Supports secondary market trades.



Market share of the top 6 NFT platforms by trading volume (as of February 2023) ⁴

Rank	NFT Marketplace	Market Share (%)
1	Blur	56.80%
2	OpenSea	36.70%
3	X2Y2	2.60%
4	Magic Eden	2.10%
5	LooksRare	1.00%
6	CryptoPunks	0.80%

Application: Adult NFTs

Through NFTs, sex workers can sell their wares through personalized videos, images, and physical objects ¹. There is a growing interest in NFT from the adult sector, which already has a reputation for being a tech pioneer. Rapper Azealia Banks sold the rights to an audio sex tape for \$17,240 ².

Each NFT is unique and it also supports trading on **the secondary market**, such as OpenSea after first produced and sold on pornographic websites. When the content is re-sold, repackaged, and reuploaded to another platform, the sex workers also **receive royalties** ¹. This serves as one factor for them to shift to NFT.

To fight sex trafficking, the Fight Online Sex Trafficking Act (**FOSTA**) and the Stop Enabling Sex Traffickers Act (**SESTA**) were signed into law in 2019 by President Trump. Both acts pose significant challenges for traditional advertising and payment methods. Many sex workers are facing difficulties in cashing out their profits. NFT thus becomes a good place to sell their products and legalize their profits since it is currently a **grey area** for adult NFT trading and profiting. Some believe the shift from traditional videos and photos to NFT is a backfire from the sex trafficking law ³, which will actually pose more challenges for regulators to trace and regulate sex trafficking.

Spank Pop Shots



Items 1834 · Created Aug 2021 · Creator earnings 10% · Chain Polygon

Collect and own a piece of pornographic history, while supporting your favorite...
See more v

6 ETH total volume 0.05 ETH floor price -- best offer 0.5% listed 218 owners 12% unique owners

Source:

1: [NFTs and Sex Workers, 2022](#)

2: [Lawrence G. Walters & Bobby Desmond, NFTs and the Legal Issues Surrounding Crypto Art](#)

3: [Eric Jame Beyer, Sex Workers Are Using NFTs to Take Control of Their Content, 2022](#)

4: [Julia Ng, Most Popular NFT Marketplaces by Market Share & Trading Volume, 2023](#)

NFT Serve as Product

What info do we have to discern any suspicious pattern?

Provided by User-KYC

Most top trending NFT platforms are anonymous for sellers and buyers. We look into the six top NFT trading platform and found in order to purchase/ sell NFT, the user only need to link the their bitcoin wallet, which is anonymous and can be set up in just one minute **without KYC process**. Users only need to create password → secure their wallets → confirm secret recovery phrase. Once connected, the platform account will be the same as wallet address.

Help us improve MetaMask

MetaMask would like to gather usage data to better understand how our users interact with MetaMask. This data will be used to provide the service, which includes improving the service based on your use.

MetaMask will...

- ✓ Always allow you to opt-out via Settings
- ✓ Send anonymized click and pageview events
- ✗ **Never** collect information we don't need to provide the service (such as keys, addresses, transaction hashes, or balances)
- ✗ **Never** collect your full IP address*
- ✗ **Never** sell data. Ever!

MetaMask is one of the most popular wallet, it doesn't collect personal info and IP address.

In some cases, user can choose to link their social media account and provide email address or phone number to the platform. All these apply to both **buyers and sellers** as long as the seller creates the NFT on the platform. **They remain anonymous in terms of proactively provide their info.**

On the right is how user can **create their NFT and become a seller**. In case where sellers may choose other blockchain and platforms to mint NFT, gas fee will be charged depends on network traffic and complexity of transactions. **Throughout the process, no KYC is required.**



Gas fee²: Gas is used to compensate miners for the computing energy and resources expended to validate transactions and to include them in the blockchain.

Collected By Platform

Besides KYC, the platform will collect information about users, which may be **identifiable and pseudonymous**. So, in terms of passively being tracked by the platform, the users are pseudonymous to some extents.

Digital Wallet: wallet balance, interactions with the Blockchain, token identifiers

Purchase activity: completed transaction hashes, information about what you purchased, from whom, the amount you paid, the cryptocurrency you used

Other: IP address, location information (including approximate location derived from IP address), clickstream data, referring/exit pages, and date/time stamps. MAC address, cookie identifiers, mobile carrier, mobile advertising and other unique identifiers, browser or device information

(Source: aggregate info from six top trading platform's privacy policy)

How to create NFT?¹



OpenSea

Upload file (JPG, PNG, GIF...)

↓
Name it, Add Description

↓
Set up explicit and sensitive content OR unlockable content

↓
Choose the number of contents to be mint

↓
Choose blockchain

↓
Finished NFT

Source: 1: [Opensea. How to create NFT](#)

2: [NFT Gas Fee: What It Is & How to Calculate It. 2022](#)

NFT Serve as Product

After understanding the KYC procedure and the information tracked by platform, we have developed an overall picture of what information the NFT trading platform may have, which will serve the foundation of assessing the platform's ability and generate suggestions to combat illegal activities such as human trafficking. Next, we will try to understand what activities are prohibited and what are platform's obligations in regulating those activities. In other words, where we previously explained **“what platform can do”** based on the information they have, here we examine **“what platforms should do”**.



What is Prohibited?

- Most platforms require users to be **18 years or older**. Location wise, users can not located in a country that is subject to a U.S. Government embargo; and are not listed on any U.S. Government list of prohibited, sanctioned, or restricted parties. What's interesting is Magic Eden¹ specifies that users can **not use any software or networking techniques, including the use of a Virtual Private Network (VPN) to modify internet protocol address** or otherwise circumvent or attempt to circumvent this prohibition.
- Other regulations **prohibit any illegal or unauthorized purpose**, including creating or displaying illegal content, such as content that may involve child sexual exploitation, encouraging or promoting any activity that violates the Terms of Service.

Source 1: [Magin Eden's Term of Service](#)



Takeaways

Using NFT to produce and trade sexual related contents is already a small niche in the market as the main purpose of NFT remains to provide a way for creators to monetize their digital creations and for other investment purposes. Within the **adult NFT sector**, it's even more challenging to identify who are the actual owner of the accounts due to the loose KYC and platforms' limited obligations to combat illegal activities. Unlike the advertisement posts, which has been around for years, adult NFT is a new area and not much red flags have been studied. So, it is going to be challenging to look for trafficker evidence in this sector.



What are they responsible for?

These platforms have explicitly state that they have **no obligation** to monitor where services are accessed from or any user that are in breach of these Terms. However, they **reserve the right**, at any time, in their sole discretion, to block access to the Services, in whole or in part, from any **geographic location, IP addresses and unique device identifiers or to any user** who they believe is in breach of these Terms.



Based on the information and right to disclose orders they have, here are some **red flags** for the platforms to watch for in the adult NFT section:

- Cross-check between IP address, wallet address, phone number and register location (if any)
- If the seller's e-mail addresses or other personal info are on the internet escort sites.
- If the seller produce different NFTs featuring many different people

Virtual Currency Serves as a Money Laundering Tool

Connection between Human Trafficking, Money Laundering & Crypto

Once trafficking happens, the imprisoned **victims** are **transported to an exploitation place** where traffickers obtain the financial proceeds¹. Instances of exploitation encompass various forms, such as sexual exploitation, including pornography and voyeuristic activities, coerced labor of any type, involuntary adoption, forced marriage, begging against one's will, and so on². With the example of exploitation, the generated **illegal profits need to be concealed or disguised before converting into legal funds**.

Therefore, any **untraceable digital asset**, such as cryptocurrency, **can be a tool to launder illegal benefits**.

Virtual Currencies:

Disguise or conceal profits



Money Laundering:

illegal profits to legal funds

Human Trafficking:

Gain Proceeds from exploitation

Case Study

DarkScandals is a **child pornography website** with a **high incidence of human trafficking**³. It started directing users to pay with pseudonymous virtual currencies like Bitcoin and Ethereum to conceal administrators' and users' identities after one year of operation.

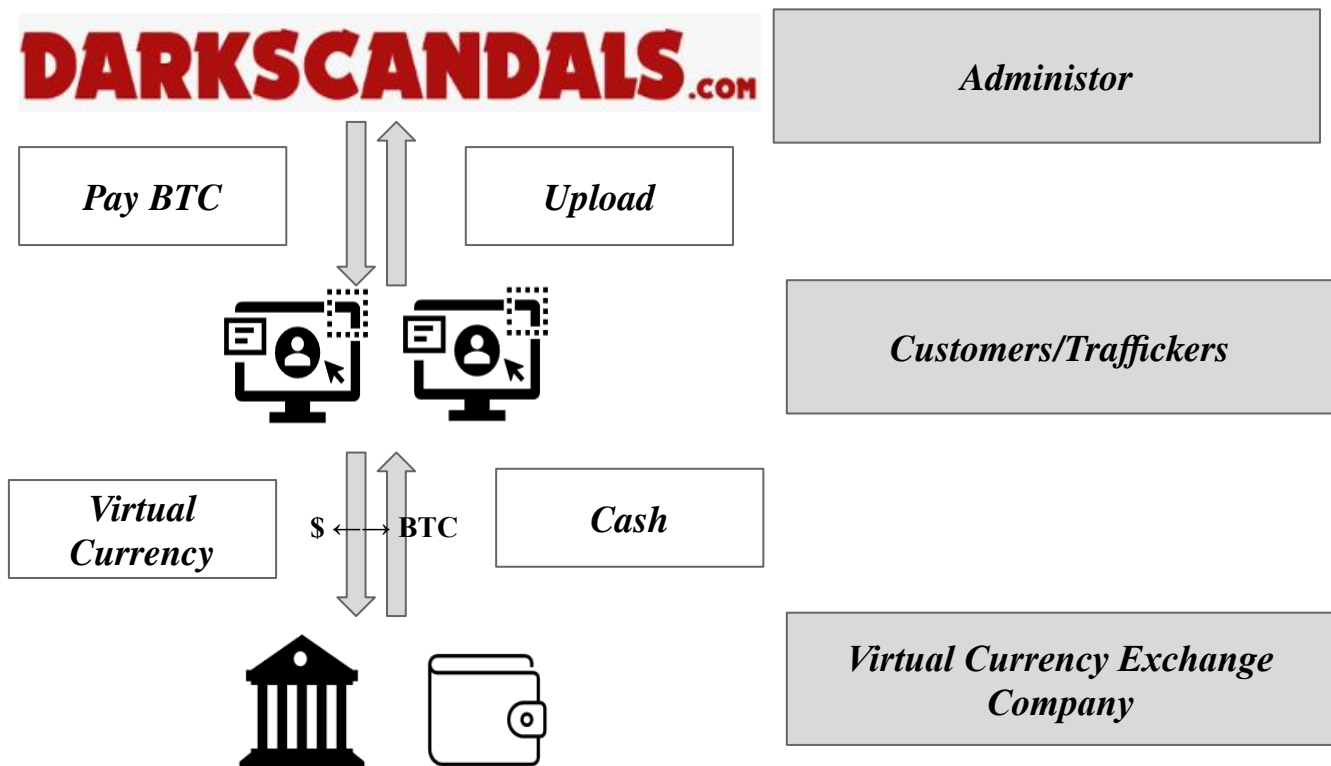
On **DarkScandals**, users had two options for accessing the content in "**packs**." They can **purchase or receive packs for free by uploading pornography videos**. To pay for packs, child sexual abuse video watchers **created accounts hosted at virtual currency companies offering cryptocurrency exchange services** (i.e., with these accounts, users can convert fiat currency into cryptocurrency and vice versa). Users paid to the address that the **DarkScandals administrator assigned**. To receive the packs, obscene video uploaders **created a virtual account with the address** to which the administrator could **send the pack** (i.e., the laundered profits).

1 & 2. Caltagir Caltagirone, S. . [The human trafficking kill chain - global emancipation network](#). GLOBAL EMANCIPATION NETWORK. P.17

3. More information can be found on The United States Department of Justice [website](#).

Virtual Currency Serves as a Money Laundering Tool

DarkScandals Transaction Pattern



Transaction Pattern Interpretation



Through the DarkScandals case, a **typical transactional pattern** shows up.

- The pattern is an **interaction between multiple users and one administrator**. To be more specific, it involves multiple customers sending Bitcoin from their individual addresses to a single address created by the DarkScandals administrator.
- The pattern requires **the use of virtual currency account hosted at exchange companies**.
- The bitcoin **address is public-listed**.

Above pattern allows transaction investigators to monitor the transactions and identify payments linked to particular virtual currency wallets by using data mining and machine-learning algorithms.

Virtual Currency Serves as a Money Laundering Tool

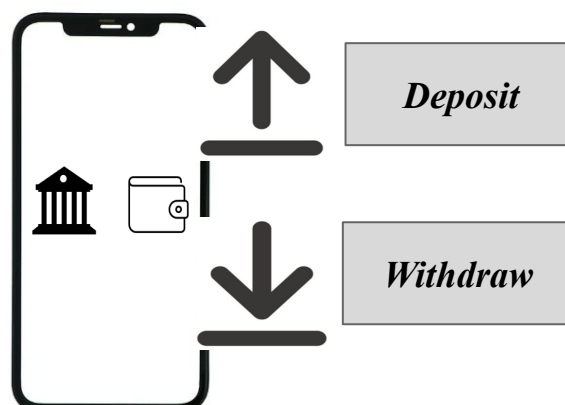
Exchange Companies' Extant Approaches to Anti Money Laundry

Approach 1: Identity Verification¹



In order to combat money laundering, various crypto exchange companies employ **different levels of due diligence measures to establish the identities of their clients, ranging from basic identity verification to multifactor authentication.** After analyzing the leading 20 cryptocurrency exchanges, our team uncovered the following discoveries.

- The **purpose** of identity verification for clients is to **obtain higher transaction limits and enhance account security.**
- The **degree of identity verification correlates with the transaction limits on digital assets.** For instance, Binance, the largest bitcoin exchange, enforces a fiat deposit and withdrawal cap of US\$50,000 for basic identity verification, while users who provide their proof of address can increase this limit to US\$200,000.
- **Verification standards differ among exchange companies.** For instance, Kraken's highest identity verification requirement mandates users to provide a legal photo ID and a selfie while holding the ID. In contrast, ByBit demands additional requirements, such as facial recognition, proof of residence issued within three months, bank statements, or utility bills.
- **All verification procedures are conducted online and may vary depending on the exchange company.**



1. Identify verification is also known as Know-Your- Customers (KYC), a required process of identifying and verifying the client's identification when creating an account and on a regular basis.

Virtual Currency Serves as a Money Laundering Tool

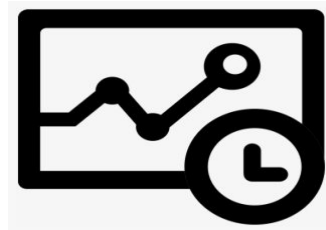
Exchange Companies' Extant Approaches to Anti Money Laundry

Approach 2: Monitoring Transaction

To ensure compliance, prevent fraudulent activities, and facilitate customer onboarding with reduced risks, a few **cryptocurrency companies employ real-time monitoring of inbound and outbound transactions on their platforms**. Our team has conducted an analysis of the KYC rules of the top 20 cryptocurrency exchanges, and has made the following observations.



First-time users



All users

→ **Virtual Assets Exchange**
Companies tend to scrutinize new users' transactions closely. For instance, Kraken imposes a **72-hour hold** on first-time digital wallet purchases and debit/credit card purchases¹. Other purchases made within the 72-hour period are also subject to hold. This approach aims **to safeguard the users' account security and mitigate the possibility of money laundering.**

→ **Digital assets trading platforms have the capability to monitor transactions and implement measures against suspicious activities.** In particular, Gate.io outlines in its user agreement that if transactions occur frequently in an account registered by the user or appear to be beyond reasonable circumstances, the company will evaluate and determine the potential suspicious nature of such transactions. Upon confirmation, Gate.io may undertake restrictive measures such as transaction suspension or denial, and may also report it to the relevant competent authorities².

1. More details can see on [Kraken O&A](#).

2. For more information, please visit [Gate.io's user agreement web page](#).

Virtual Currency Serves as a Money Laundering Tool

Underlying Problems of Extant Approaches & Takeaways

Problem 1: Cryptocurrency exchange companies employ different standards when it comes to KYC procedures, ranging from loose to strict because the regulatory framework for virtual currency exchanges also vary depending on the jurisdiction. Some exchange companies may implement the lowest possible KYC standards within the existing legal framework. This reluctance to implement more rigorous KYC policies is often due to concerns about discordance with the fundamental principles of blockchain platforms, which prioritize decentralization.

1, The Financial Crimes Enforcement Network is a bureau of the US Department of the Treasury that gathers and analyzes financial transactions to combat domestic and international money laundering and other financial crimes

Problem 2: Despite the ability of virtual assets exchange companies to monitor transactions and take action against suspicious activities, there is still a gap in their capacity to link suspicious transactions with cases of human trafficking. It is important to note that a transaction that appears suspicious does not always indicate potential human trafficking. Furthermore, technical personnel within the risk compliance department may lack the expertise to identify cases of human trafficking.

Problem 3: The implementation of KYC measures taken by exchange companies is primarily driven by self-interest and the need to protect their operations. Gate.io, for instance, explicitly states on its website that users are solely responsible for ensuring that their access to the site and use of the company's services comply with relevant local laws and regulations. This disclaimer absolves Gate.io of any legal ramifications resulting from users' failure to comply with applicable laws and regulations.

- **FinCEN¹ can conduct a review of the current registration requirements for money service businesses that operate virtual currency exchange businesses.** Given the nature of virtual currency, decentralization and pseudonymity, FinCEN can develop new KYC solutions that are better aligned with the principles of blockchain platforms, with the collaboration experts in the field.
- Virtual currency exchange transactions can **undergo more regular audits** to ensure the proper implementation of KYC procedures and to identify any potential compliance violations.

- To address the gap in identifying human trafficking transactions in cryptocurrency exchanges, **organizations with expertise in this area can establish a private-public partnership with the operational exchange companies.** For instance, the Financial Action Task Force has provided red flag indicators for virtual assets to help identify potential cases of trafficking. Through a cyclical and evolutionary process that considers the unique risks and contexts of a jurisdiction, customer type, or reporting entity, this information from operational agencies can be developed further.

- Considering the tendency of virtual currency exchange companies to refrain from acting as whistleblowers, **regulatory authorities should adopt a proactive approach and seek the cooperation and assistance of such companies when identifying instances of human trafficking through cryptocurrency transactions.**

Conclusions

The objective of these four case studies **is to provide insight into how digital assets are employed throughout the entire process of human trafficking, and to identify the evidence that can be used to detect such activities.** As evidenced by four cases, the utilization of digital assets is instrumental in facilitating human trafficking. This includes the purchase of third-party platforms using cryptocurrencies to post advertisements and attract potential buyers, as well as the creation of their own platforms using blockchain technology. Furthermore, traffickers may employ NFTs to circulate sexual contents and profit from the exploitation of victims, as well as engage in the final step of money laundering. In light of these examples, it is clear that digital assets play a critical role throughout the whole process of human trafficking.

After understanding the roles and levels of involvement of digital assets associated with human trafficking, **we proceed to search for evidence to identify human trafficking.** We hold positive attitudes toward discovering evidence in identifying human trafficking in the ad space given it has been a traditional method to profit from human (sex) trafficking and extensive studies have generated red flags for regulators to watch out: trustworthy provider language, obscured phone number, provider ethnicity and language suggesting youth. However, due to the constantly evolving nature of these activities, institutions must continually develop new tools to identify and prevent trafficking through advertisements.

When considering the use of pornographic sites and adult NFT trading in the context of human trafficking, **there are several challenges to identifying whether the owners and content creators are sex workers or sex traffickers.** These challenges include the loose KYC procedures, limited obligations of the platforms to combat illegal activities, and the fact that these are newly emerging trends compared to traditional advertising. Therefore, we believe enhancing KYC is the fundamental step in monitoring suspicious transactions and preventing human trafficking. In addition, some NFT trading platforms will collect user information, which can be utilized to identify suspicious accounts. One method is cross-checking multiple data points such as IP address, wallet address, phone number, and registered location (if available) to verify if they match up. Additionally, platforms can compare the seller's email addresses or other personal information with information found on internet escort sites to see if there is a match. Another approach could be to monitor whether the seller produces different NFTs featuring many different people, if so, it's unlikely that the account owner is simply a sex worker. Besides these efforts, it is essential to balance the need to protect the rights and safety of sex workers while also working to eliminate trafficking activities.

Conclusions

Although **virtual asset exchange companies** do implement KYC procedures to verify the identities of users and monitor their transactions, these companies **may vary in the stringency of their KYC standards, as they are driven by the need to protect their own interests**. Furthermore, there remains a gap in the ability of these companies to link suspicious transactions with cases of human trafficking. To address the issues related to human trafficking facilitated by digital assets, government authorities can review the existing legal framework and develop new KYC solutions that are better aligned with the principles of blockchain platforms. In addition, regulatory authorities can conduct more frequent audits of virtual currency exchange transactions to ensure compliance with KYC procedures. In the end, regulatory authorities should adopt a proactive approach and seek cooperation and assistance from organizations in this area through public-private partnerships.

The use of digital assets has emerged as a persistent trend in the context of human trafficking, posing a significant challenge to identifying such illegal activities. However, there's still evidence that regulators and organizations can pay attention to. Thus, we acknowledge that there are **both challenges and opportunities** in combating human trafficking from the digital assets approach. We remain optimistic about the prospects of finding better solutions to combat human trafficking in the digital world. With ongoing advancements in technology, we believe that there is potential for more effective strategies to be developed that can help to prevent and detect human trafficking activities, as well as provide support and assistance to victims. It is crucial to continue exploring and implementing innovative approaches to address this pressing issue.

Thank you!

For questions, contact us:

Jingyun Yu jy668@cornell.edu
Puiman Shing ps862@cornell.edu
Qian (Rebecca) Liu ql266@cornell.edu
Tianchang (Shirley) Wang tw525@cornell.edu

