Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies Phase III

Examining the effects/implications of CBDCs, AI, and Zero-Knowledge Proofs in the cyber-fraud space along with other current trends and recent case rulings

2024 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Abstract

Over the past 3 years a sector that has been rapidly developing is the use of digital assets and their correlation to illicit activity. In the previous two cycles of the AEP program, the group of Combating Illicit Activity Utilizing Financial Technologies and Cryptocurrencies seeked to provide great research into the use of digital assets and emerging financial technologies in criminal activities and how to effectively combat criminal activity in this space. This team decided to do one final concluding phase to address some areas that were briefly touched on not addressed in the previous two cycles. These include central bank digital currencies, zero-knowledge proofs, AI influence on cyber-financial crimes, current/updated trends in the digital asset space, and recent rulings that have shaped the future of punishments for cyber-financial crimes. The key to combating criminal activity in the digital asset space and among emerging financial technologies is raising awareness of it and informing stakeholders just how far-reaching it can be which the previous 2 phases have accomplished but we always aim to reach a larger audience. We seek to continue arming our colleagues, constituents, and general consumers with increased knowledge in this space.

Homeland Security

2024 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Team Introductions

MEMBERS	COMPANY/AGENCY
Champion: Stephen Deininger	**NSA**
Kevin Lyons, Sec+, CFE	**U.S. Secret Service**
Mattonna Wahlgren, CFCS	**Evolve Bank & Trust**
Heather Jones	**DoD**
Julia Maguire	**Citibank**
Jon McWilliams	**FBI**
Susan Shaffer	**Quad City Bank & Trust**

Homeland Security

2024 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Table of Contents

Homeland Security

Central Bank Digital Currencies & The Implications of Issuing CBDCs

Advantages and Disadvantages of CBDCs

Central bank digital currencies (CBDCs) present both opportunities and risks. They have been a hot topic for years as digital currency has become more ingrained in modern payment systems and more accepted by the general public. Multiple countries around the world are already piloting CBDCs or are in the active development of CBDCs. Though they possess a fair amount of benefits on the surface, it is important to turn attention to the risks they employ. CBDCs can have a direct correlation to the cyber-fraud space and illicit actors. Here are some of the potential risks associated with CBDCs:

Systemic Risk: Introducing a CBDC could pose systemic risks to the financial system if not properly managed. It could potentially lead to bank runs as individuals might prefer holding their funds in the central bank rather than commercial banks, especially during times of economic uncertainty.

Privacy Concerns: CBDCs could raise privacy concerns as central banks would have access to detailed transaction data of individuals. Depending on how the CBDC is designed, this could lead to potential surveillance or invasion of privacy issues.

Cybersecurity Vulnerabilities: CBDCs could be susceptible to cyber-attacks, hacking, and other security breaches. Any compromise in the system's security could lead to financial losses for individuals and disrupt the stability of the financial system.

Operational Challenges: Implementing and managing a CBDC would require significant technological infrastructure and expertise. Central banks would need to ensure the reliability and efficiency of the CBDC system to prevent operational disruptions.

Monetary Policy Transmission: CBDCs could potentially alter the transmission mechanism of monetary policy. If individuals shift their preferences from bank deposits to CBDCs, it could affect the effectiveness of traditional monetary policy tools such as interest rate adjustments.

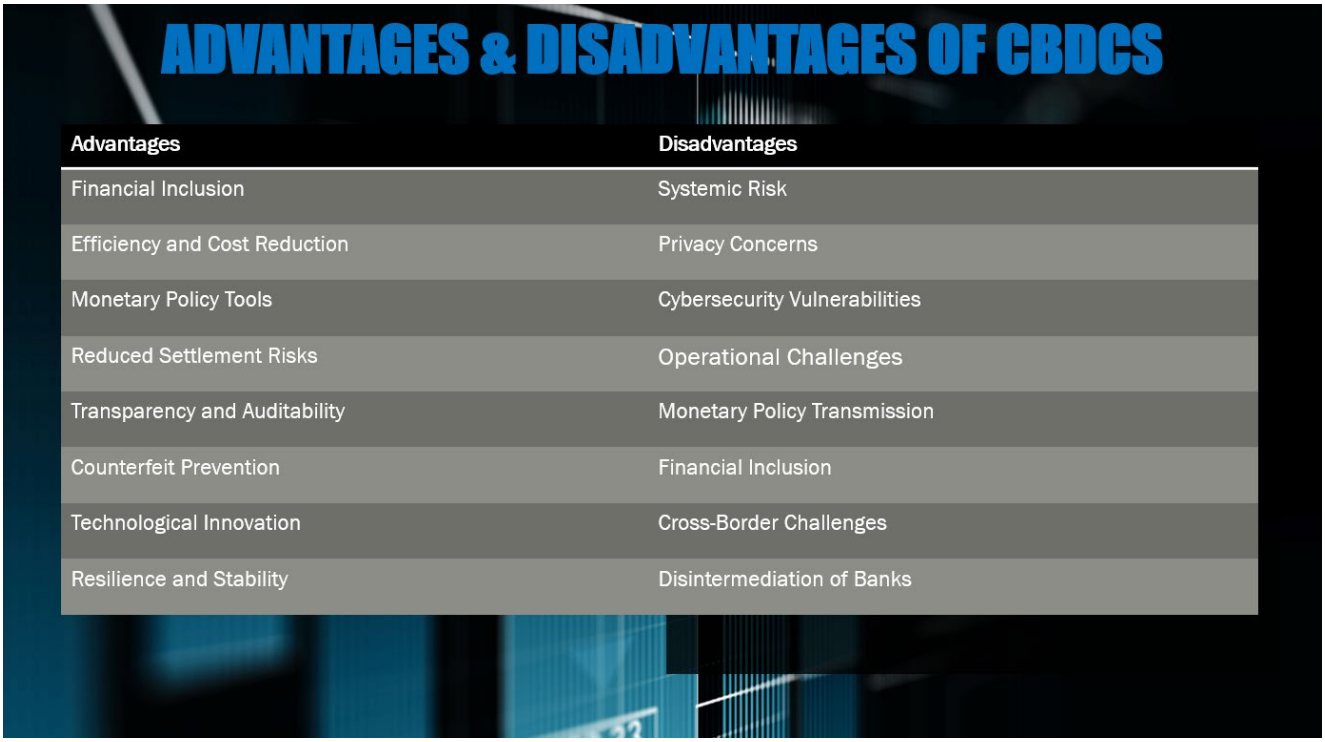
Financial Inclusion: While CBDCs have the potential to improve financial inclusion by providing access to banking services for the unbanked population, there's a risk that those without access to digital devices or the internet could be further marginalized.

Cross-Border Challenges: Coordinating CBDCs across different jurisdictions could pose challenges, especially regarding regulatory compliance, interoperability, and exchange rate management.

Disintermediation of Banks: CBDCs might lead to disintermediation, where individuals bypass commercial banks and directly hold funds with the central bank. This could undermine the traditional banking system's role in credit creation and financial intermediation.

Legal and Regulatory Risks: Introducing CBDCs would require significant legal and regulatory frameworks to address issues such as anti-money laundering (AML), counter-terrorism financing (CTF), and consumer protection.

International Reserve Currency Status: The introduction of CBDCs by major economies could potentially challenge the dominance of existing international reserve currencies like the US dollar, leading to geopolitical tensions and economic uncertainties.[12]



Addressing these risks would require careful design, regulation, and international cooperation to ensure the successful implementation of CBDCs while mitigating potential adverse effects on financial stability, privacy, and monetary policy.

Adopting central bank digital currencies (CBDCs) can offer several potential benefits, which vary depending on the design and implementation of the CBDC. Some of the key benefits include:

Financial Inclusion: CBDCs have the potential to improve financial inclusion by providing access to banking services for individuals who are currently unbanked or underbanked. Digital currencies can reduce barriers to access financial services, especially for marginalized populations who may lack access to traditional banking infrastructure.
Efficiency and Cost Reduction: CBDCs can streamline financial transactions, reducing the costs and time associated with traditional payment methods. Digital currencies can

facilitate instant peer-to-peer transactions, cross-border payments, and micropayments, leading to increased efficiency in the financial system.

Monetary Policy Tools: CBDCs can enhance the effectiveness of monetary policy by providing central banks with new tools to manage the money supply and interest rates. Digital currencies enable more direct and precise control over the circulation of money, allowing central banks to implement monetary policy more effectively to achieve macroeconomic objectives such as price stability and full employment.

Reduced Settlement Risks: CBDCs can mitigate settlement risks in the financial system by enabling real-time gross settlement (RTGS) of transactions. Digital currencies settle transactions instantly, reducing the need for intermediaries and the risk of counterparty default.

Transparency and Auditability: CBDCs offer increased transparency and auditability compared to cash and traditional banking systems. All transactions recorded on the blockchain, or distributed ledger can be traced and verified, enhancing the integrity of the financial system and reducing the risk of fraud and corruption.

Counterfeit Prevention: CBDCs can help prevent counterfeit currency and illicit activities such as money laundering and terrorist financing. Digital currencies incorporate advanced encryption and security features, making them more resistant to counterfeiting and unauthorized duplication.

Technological Innovation: The adoption of CBDCs can drive technological innovation in the financial sector, spurring the development of new financial products and services based on blockchain technology and distributed ledger technology (DLT). CBDCs can also promote interoperability and standardization in the digital currency ecosystem, fostering collaboration among stakeholders.

Resilience and Stability: CBDCs can enhance the resilience and stability of the financial system by diversifying the payment infrastructure and reducing reliance on centralized intermediaries. Digital currencies are less vulnerable to systemic risks such as bank failures and liquidity shortages, enhancing financial stability in times of crisis.[34]

Overall, CBDCs have the potential to transform the global financial system, unlocking new opportunities for economic growth, financial inclusion, and innovation while addressing existing challenges and inefficiencies. However, realizing these benefits requires careful design, regulation, and collaboration among policymakers, central banks, and other stakeholders.

Uses of CBDCs in Illicit Activity

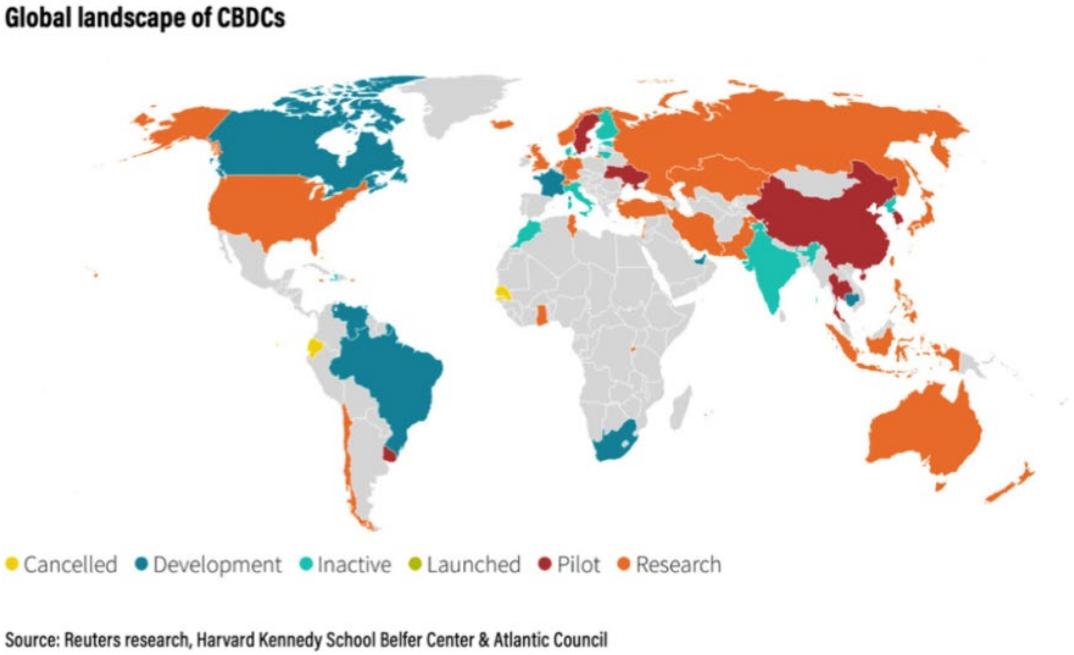
Central bank digital currencies (CBDCs) have the potential to be misused in criminal activities, much like traditional fiat currencies and digital currencies such as cryptocurrencies. Here are some ways in which CBDCs could potentially be used in criminal activity:

Money Laundering: Criminals could use CBDCs to launder money by transferring illicit funds through anonymous transactions facilitated by the digital currency. CBDCs could provide a convenient and relatively anonymous means of moving large sums of money across borders without the need for intermediaries.
Terrorist Financing: CBDCs could be used to finance terrorist activities by providing a secure and relatively untraceable method of transferring funds between individuals and organizations involved in illicit activities.
Fraudulent Activities: Criminals could exploit CBDCs to engage in various forms of fraud, such as creating counterfeit digital currency, conducting phishing scams, or manipulating digital currency exchange rates for financial gain.
Black Market Transactions: CBDCs could facilitate transactions on illicit online marketplaces, such as darknet markets, where illegal goods and services are bought and sold anonymously. Criminals could use CBDCs to purchase drugs, weapons, stolen data, and other illegal items.
Ransomware Payments: Criminals behind ransomware attacks could demand payment in CBDCs to unlock encrypted files or systems. CBDCs could provide a convenient and relatively anonymous means of transferring ransom payments without the need for traditional banking channels.
Extortion and Cybercrime: Criminals could use CBDCs to extort money from individuals or organizations by threatening to release sensitive information, launch cyberattacks, or disrupt critical infrastructure. CBDCs could facilitate payments in exchange for silence or protection against further harm.
Corruption and Bribery: CBDCs could be used to facilitate corrupt practices, such as bribery, embezzlement, and kickbacks, by providing a secure and relatively untraceable means of transferring funds between corrupt officials and individuals seeking favors or preferential treatment.

Tax Evasion: Criminals could use CBDCs to evade taxes by conducting transactions off the books or hiding assets in digital wallets outside the reach of tax authorities. CBDCs could enable individuals and businesses to conceal income, profits, and assets from taxation.[56]

U.S. Adoption of CBDCs

The United States had not yet adopted a central bank digital currency (CBDC). However, discussions and research regarding the potential issuance of a digital dollar are ongoing within various government agencies, including the Federal Reserve. The Federal Reserve and other U.S. authorities have been closely monitoring developments in the digital currency space, including the rise of private cryptocurrencies like Bitcoin and stablecoins. There have been several hearings and discussions in the U.S. Congress regarding the potential benefits and risks of CBDCs. The below map shows the current state of adoption of CBDCs across the globe. A few countries have implemented a pilot program and it will be key for the U.S. to pay attention to these developing countries for any future movement in the space.[78]



Effects of AI on Digital Asset Related Crimes and Cyber-Financial Crime

What are the effects of AI on Digital Asset Crime and Cyber-Financial Crime?

What exactly is artificial intelligence (AI)? AI is in the simplest term, a machine's ability to combine computers, datasets and sets of instructions to perform tasks that usually require human intelligence, such as reasoning, learning, decision-making and problem-solving. AI can

be categorized as a general-purpose tool, meaning it can be used for almost every task. And like every general-purpose tool, cybercriminals may use AI for malicious purposes as well.[1]

There is no doubt that the development of AI has brought with it a huge range of benefits to many businesses. In the last decade, the significant increase in the adoption of AI and machine learning (ML), has enabled a number of organizations to successfully harness these technologies and implement them into their business practices, streamlining processes and improving productivity.[2]

Today, businesses across almost every sector are looking for the opportunity to incorporate AI in support of their operations. However, as with any industry, the advancements of AI have brought with it a darker side to the technology. The advancement of AI has not only brought improvements to the business sectors; but it has also brought improvements in the illicit actions of fraudsters. For example, generative AI has allowed for increasingly sophisticated technologies to write malicious code and highly convincing phishing emails.

Further, AI has been utilized to enhance existing forms of attack, such as utilizing AI skills to create more convincing phishing emails making it difficult for SPAM filters and antivirus software to identify malware. Additionally, it has provided individuals better skills for creating fake data which leads to impersonations. It has also allowed for larger scale attacks to be completed with little effort.

Top AI crimes impacting Digital Asset Crime and Cyber-Financial Crime

With the increased sophistication of many AI tools, as well as the open access to many of them, they have created a landscape where many AI tools can be utilized for both positive and negative use. Further, as the creators of AI continue to develop their skills, more and more of these tools become user friendly which require less skill on the user end. This has allowed for a situation to develop where people of all ages and locations are now able to utilize AI tools for both licit and illicit activity. Furthermore, some AI tools which have been developed for licit use are now able to be utilized for illicit activity. The more user friendly the AI tools are becoming the more these tools are available for use by individuals across all ages and skill sets. This availability has allowed for these AI tools to be more impactful in a range of activities from creating AI and cyber based frauds to hacking. In addition to being more impactful, this user friendliness has also allowed these crimes to have far reaching effects and crossover multiple crime categories.

In a world of generative AI, we are seeing the Know Your Customer (KYC) impact through the use of synthetic and/or stolen IDs as well as AI generated KYC ``selfie" images and/or videos. As generative AI has become more user friendly, we are seeing that generative

AI can create bogus documents quickly and on a massive scale.[3] An online article posted on Payment Village walks users through the process of creating deepfakes using both DeepFace Lab and Deepfake Offensive Toolkit. The writer of the article posted the images and indicated the steps required as well as the issues identified with each refined deepfake as he attempted to bypass the KYC banking requirements.[4] Ultimately, though the process was conducted with some trial and error, he was successful in creating a deepfake which passed the KYC measures. As shown in this article, while some information is being provided for licit and training purposes, that same information is now available for illicit use as well. For those who are less interested in making their own deepfakes to bypass KYC, it is reported that deepfake IDs can be purchased for as little as $15 online and are being used to bypass KYC requirements for some cryptocurrency exchanges. In some cases, allegations are made that sites such as OnlyFake sell deepfake IDs which have been lauded to bypass KYC requirements for institutions ranging from Revolut to Kraken.[5] According to the BioCatch's 2024 AI, Fraud, and Financial Crime Survey, 72% of respondents said their organization faced cases of synthetic identities when onboarding new clients.

One of the increasing concerns associated with generative AI models and KYC, is the potential for generative AI through the use of large language models (LLMs) to create deep back stories for their frauds which could pass the scrutiny of a standard banking or employee KYC review. Further, as remote work has become a staple in some industries there are concerns that individuals could perpetrate payroll fraud through the use of these deepfake back stories to obtain employment as a remote employee and draw payroll from multiple companies at one time.[6]

A review of the top cyber-financial crimes which are being conducted utilizing AI revealed crimes primarily identified as fraud and cyber crimes. The fraud style crimes include notable frauds such as spoofing, phishing, spear phishing, and whaling. These fraud crimes are identified as being completed via private and business email as well as via SMS-text messaging.[7] The cyber style crimes are identified as being Deepfakes, password cracking, hacking, and supply chain attacks.[8]

These types of crimes have a far-reaching effect not only to the direct victim of the crime, but in some cases on other individuals as well. For example, with the increased skill of AI, individuals with little to no skill are now in a position to create fake data which can allow for the impersonation and/or exploitation of others. AI tools have allowed for the ability to craft not only written, but also audio and visual "deep fakes" which can be difficult to distinguish as false. In recent months, we have seen this phenomenon utilized in the circulation of deep fake pornography created with the attributes of pop singer Taylor Swift. This process was also utilized to trick a UK-based energy firm into transferring €220,000 to a Hungarian bank account

in 2019.[9] Both of these instances reflect the far-reaching damage which can be done through this type of AI assisted cybercrime.

How have the improvements in AI enhanced crimes of spoofing, phishing, and impersonation in Digital Asset Crime and Cyber-Financial Crime

Criminals have used AI to more effectively commit crimes. Here, we will discuss how criminals use AI to phish, spoof and impersonate to prey on their victims.

Phishing

Cybersecurity professionals have voiced concern how AI could make phishing emails more of a problem. Oftentimes, phishing emails can be easy to detect. Indicators of phishing emails are spelling errors, bad grammar and mis-capitalized words.[1] AI could be used in such a way that these traditional indicators are either obsolete or more difficult to detect which can make phishing emails all the more attractive method for criminals to commit fraud. In addition to the fraud component, this can pose a greater challenge for cybersecurity departments. As AI language capabilities improve, it will also make the phishing emails more human like which can in turn, make the emails more difficult to detect.[2]

AI is used to create both phishing and spear-phishing email. This method makes phishing/spear-phishing cheaper and more effective for criminals. Ai can be used to create highly realistic emails directed at specific individuals and as a result, the success of phishing/spear-phishing may increase. According to a study by the Harvard Business Review, AI generated phishing emails were 95% cheaper than non-AI generated phishing emails.[3]

Spoofing and Impersonation Scams

AI has been used to commit spoofing and/or impersonation scams. This type of scam can take different forms. One way is for AI to be used to impersonate or "spoofing" a friend or family member. This can be done in conjunction with AI spoofing of a phone number of a friend or family member.[3] What can occur is that a phone call comes to an individual who believes someone they know is calling them since the voice of the friend or family member will sound familiar. The person may describe a serious situation and request money be sent. In reality, the whole call is a scam and the person who answered the call sends money to a fraudster, not a friend or family member.

In California, companies used AI generated videos of business CEOs as part of their fraud scheme. The fraudsters used the AI generated video of a CEO to tout a company's "profitability."[4] It turned out that the actual CEO was not in the video.

Another variation of an impersonation scam is where a fraudster may pose as a government investigator with an agency such as the IRS.[5] The fraudster may demand that the victim send them cash or cryptocurrency. While this version of an impersonation scam may not always use an AI generated voice, it is still a financial scam that could easily incorporate AI generated voices or videos.

Is there a path forward? What can we do?

The use and challenges of AI are vast and wide ranging. While it is unclear where the result of AI will be in the future, currently there is a path forward for how it can be implemented now and how the potential resulting harm can be mitigated. There are two ways the negative impacts of AI could be mitigated. The first is that the private sector can take steps to mitigate AI abuse. The private sector could use AI to mitigate AI abuse. The second way AI could be safeguarded is through government legislation or regulation. There may be opportunities for regulations similar to or modeled on financial reporting requirements or other compliance regimes. Compliance certainly comes with cost, both in personnel and financial resources. However, unchecked AI abuse also comes with a cost. There needs to be a balance of an AI regulation regime that is also not overly burdensome.

Private Sector

There are steps that can be taken by the private sector to mitigate AI financial fraud. For example, financial institutions can implement a version of multi-factor authentication. This could include a fingerprint, PIN or text verification for activity that may be a deviation from normal activity.[1] While this may be imperfect it could substantially mitigate the negative impacts of AI fraud.

The good news is that while threat actors have harnessed the power of AI in their illicit activity, non-threat actors can take advantage of AI to protect themselves and their clients. There are private sector entities that are using AI to combat illicit use of AI. There is the possibility to use generative AI such as ChatGPT if integrated correctly to combat AI.[2,3] AI could be used to detect suspicious activity by comparing current activity with past activity. The use of Machine Learning algorithms could go a long way to assist in identifying potential fraudulent activity that is a result of scams-whether AI driven or not.[4] AI could be used to identify fraudulent practices and bad actors by increasing the types of data used in fraud prediction models, computer vision for ID document analysis, logins that identify voice identification, and natural language processing to monitor changing activity of individuals and organizations.[5] The use of Large Language Models (LLM) could help identify phishing emails.[6] The use of AI to scan and identify emails could help mitigate the effects of both non-AI and AI generated phishing/spear-phishing emails.

Government Regulation

Government at the federal and state level may have an interest in adopting legislation that requires financial institutions to have compliance requirements showing that they are taking steps to mitigate AI fraud While compliance regulations come at a cost both financially and otherwise, it may benefit private sector entities to support an AI regulation regime as they may be able to mitigate financial loss and suffer less reputational harm if they demonstrate they are taking steps to mitigate AI fraud.

The US Government has hinted towards some form of AI regulation. In October 2023, the White House issued an Executive Order that stated the President's Administration would "engage with international allies and partners in developing a framework to manage AI's risks, unlock AI's potential for good, and promote common approaches to shared challenges."[7] The United States Government may be prompted to act in some way due to legislative action being taken by the European Union (EU) According to its Digital Strategy, the EU wants to "regulate artificial intelligence (AI) to ensure better conditions for the development and use of this innovative technology. AI can create many benefits, such as better healthcare; safer and cleaner transport; more efficient manufacturing; and cheaper and more sustainable energy."[8] The legislation requires assessment-based levels of risk related to different types of AI capabilities and it requires transparency.[9] US based legislation could incorporate some or all of these parameters.

According to the Council of State Governments, since 2019, 17 states have enacted 29 state laws directed at AI regulation.[10] Most of these state level laws are directed at protecting individuals and requiring transparency in the development and application of AI. One of the challenges of any of these laws is how they are enforced. There are many gaps and lack of clarity regarding many policies regarding how AI is developed and used.

While AI specific legislation is likely needed, there may be an intermediate solution where current laws and regulations may be able to be used to mitigate some negative AI activity. In April 2023, several US federal government agencies issued a joint statement stating that "existing legal authorities apply to the use of automated systems and innovative new technologies."[11] For example, in February 2024, the Federal Communications Commission applied restrictions in the Telephone Consumer Protection Act on AI-generated voices.[12] This could be a blueprint for regulators to be creative in how current laws could be used but still follow the spirit of the law.

Zero Knowledge Proofs

What are Zero Knowledge Proofs and What Risks are Associated With Them?

Zero-knowledge proofs (ZKPs) are a cryptographic technique used to prove the validity of a statement without revealing any information beyond the validity of the statement itself. Zero Knowledge Proofs allow crypto network users to verify the validity of a transaction without revealing details of the transaction. While ZKPs offer significant advantages in terms of privacy and security, they also come with certain risks and limitations. Some of the risks associated with zero-knowledge proofs include:

Complexity: Zero-knowledge proofs often involve complex cryptographic algorithms and mathematical concepts, which can be difficult to implement and verify correctly. Errors or vulnerabilities in the implementation of ZKP protocols could compromise their security and privacy guarantees.

Performance Overhead: Zero-knowledge proofs typically require significant computational resources to generate and verify, which can introduce performance overhead in practical applications. The computational cost of ZKPs may limit their scalability and applicability in real-world scenarios, particularly for large-scale systems with high transaction volumes.

Trusted Setup: Certain types of zero-knowledge proofs, such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), require a trusted setup phase during which a trusted party generates initial parameters. If the trusted setup process is compromised or manipulated, it could undermine the security of the entire ZKP system, potentially enabling malicious actors to create false proofs.

Soundness Assumptions: The security of zero-knowledge proofs relies on certain mathematical assumptions, such as the hardness of discrete logarithm or factoring problems. If these assumptions are proven false or if new cryptographic attacks are discovered, it could weaken the security of ZKPs and render previously generated proofs invalid.

Privacy Risks: While zero-knowledge proofs provide strong privacy guarantees for the prover, there may still be privacy risks associated with other aspects of the system, such as the metadata associated with transactions or the potential for side-channel attacks. Care must be taken to address these privacy risks comprehensively when deploying ZKP-based systems.

User Experience: Zero-knowledge proofs can introduce additional complexity and friction into user interactions, particularly if users are required to generate or verify proofs as part of their interactions with a system. Poorly designed user interfaces or cumbersome workflows could deter users from adopting ZKP-based systems.

Regulatory and Compliance Challenges: Zero-knowledge proofs may pose challenges in terms of regulatory compliance and legal frameworks, particularly in regulated industries such as finance and healthcare. Regulatory authorities may require transparency and auditability, which could be at odds with the privacy guarantees provided by ZKPs.[12]

Advantages of Zero Knowledge Proofs and How They Could be Utilized for Illicit Activity?

Despite these risks, zero-knowledge proofs offer significant potential benefits in terms of privacy-preserving authentication, verifiable computation, and secure multi-party computation. As cryptographic techniques continue to evolve and improve, addressing these risks will be crucial to unlocking the full potential of zero-knowledge proofs in various applications.

While ZKPs have numerous legitimate applications in privacy-preserving authentication, verifiable computation, and secure multi-party computation, they could also potentially be misused in criminal activities. Here are some ways in which zero-knowledge proofs could be used in crime:

Anonymous Transactions: Zero-knowledge proofs could be used to facilitate anonymous transactions in illicit markets, such as darknet marketplaces, by providing cryptographic guarantees of transaction validity without revealing the identities of the transacting parties or the details of the transactions.

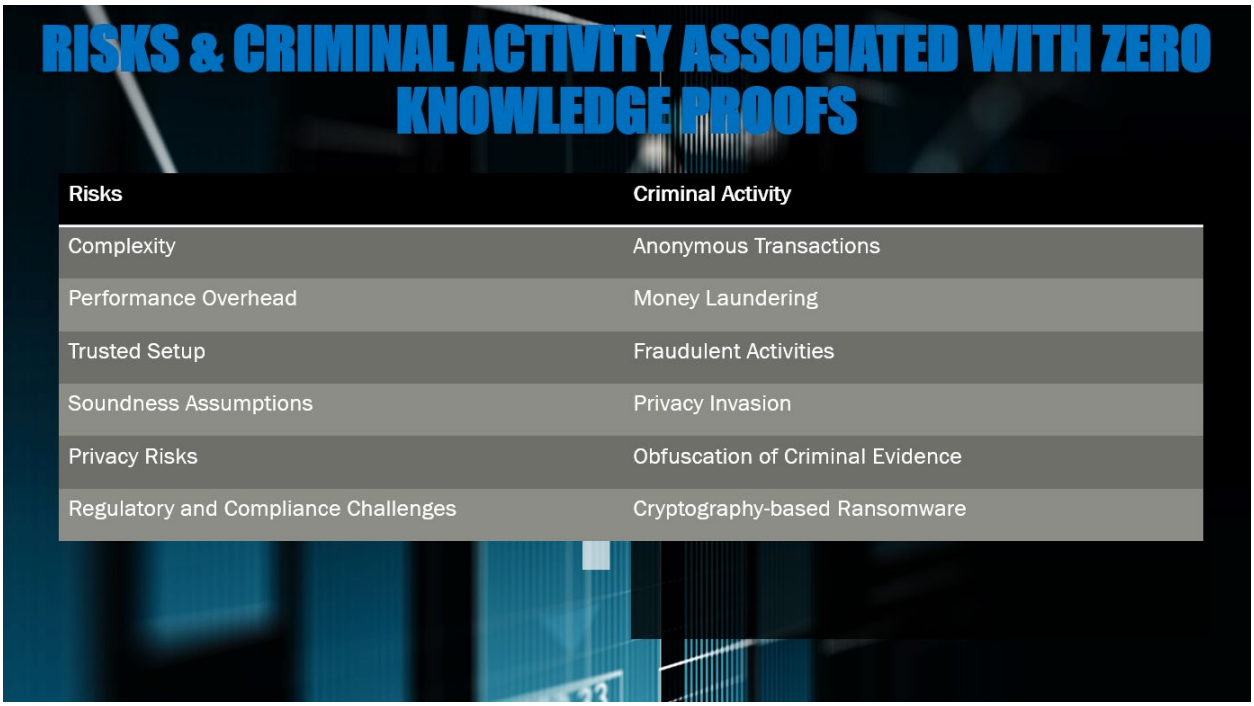
Money Laundering: Criminal organizations could use zero-knowledge proofs to obscure the origins and destinations of illicit funds by providing cryptographic proofs of the legitimacy of transactions while hiding the underlying financial trail.

Fraudulent Activities: Zero-knowledge proofs could be used to create fraudulent proofs of ownership or authenticity in various contexts, such as counterfeit product verification or fraudulent asset transfers, by generating convincing cryptographic evidence without actually possessing the legitimate credentials.

Privacy Invasion: While ZKPs are designed to protect privacy, they could also be misused to invade privacy by providing cryptographic proofs of sensitive information or activities without the consent of the individuals involved, such as unauthorized surveillance or data breaches.

Obfuscation of Criminal Evidence: Zero-knowledge proofs could be used to obfuscate or tamper with digital evidence in criminal investigations by providing cryptographic proofs of altered or fabricated data without leaving traceable trails of manipulation.

Cryptography-based Ransomware: Criminals could employ zero-knowledge proofs as part of ransomware attacks, using cryptographic techniques to encrypt victims' data and provide proofs of decryption capability in exchange for ransom payments without revealing the decryption keys or compromising their anonymity.[34]



Zero-knowledge proofs directly correlate to privacy coins and therefore the great risks that privacy coins deploy. Privacy coins like Monero and Zcash use zero knowledge proofs to cloak users' transactions. As addressed in previous phases of the program, privacy coins pose the greatest danger for illicit activity use. Use of privacy coins is increasing as the law enforcement community and general public becomes more knowledgeable on tracing multiple forms of cryptocurrencies. Regulatory oversight, enforcement mechanisms, and technological safeguards are essential for addressing the risks associated with the misuse of zero-knowledge proofs in crime.[5]

Current Trends in Digital Asset Space

Human trafficking and the dissemination and creation of Child Sex Abuse Materials ("CSAM") are among the current trends in the illicit digital assets space. According to the 2024 Chainalysis Crypto Crime Report, "CSAM is an understudied part of the crypto crime ecosystem."[1] This is due to reasons such as the industry having a focus on trading material without involving the use of currency at all, the prohibition of the sale of the material on

darknet markets, or failure to advertise due to the nature of the activity. However, as also noted in this report "…Cryptocurrency-based sales of CSAM are a growing problem…virtual currency is the dominant choice for buyers and sellers of commercial child sexual abuse content, so much so that [the Internet Watch Foundation] now have a dedicated crypto unit that works with law enforcement and the finance industry to help provide evidence for investigations.'"[2] Therefore, it is imperative that we remain vigilant in trying to identify and disrupt this activity in the digital asset space.

Human Trafficking takes on several different forms in relation to the digital asset space. Human trafficking involves "the use of force, fraud, or coercion to obtain some type of labor or commercial sex act."[3] There are millions of people all over the world that fall victim to trafficking each year. There is a newly emerging area of human trafficking that is directly linked to Cryptocurrency scams that are targeting people worldwide and that is responsible for stealing billions in funds from its victims. This trafficking is occurring in Myanmar and Thailand to fuel pig butchering operations. There are compounds that have been built to hold victims of this abuse and to further support these operations. These operations have significantly grown in size, and sophistication over the past couple of years, and definitely deserves the attention of law enforcement and the private sector to disrupt the activity.

CSAM

In the FI industry, anti-money laundering ("AML") and financial crimes analysts rely on certain typologies to identify and flag funds related to CSAM flowing through their institutions. One red flag that is important and provides many leads is the use of cryptocurrency exchanges, as on and off boarding ramps of fiat currency, to trace money flowing through these institutions. Investment in cryptocurrency tracing tools is imperative to this analysis and to monitor the risk that an institution's own customers are using their accounts to fund cryptocurrency wallets in order to conduct this type of high-risk behavior. These tools include Chainalysis, which is known for its intense study of, and vetting of, wallets and transactions to be able to label wallets as related to certain exposure for high-risk activity, with almost near certainty, including wallets related to CSAM. For instance in their 2024 crypto crime report Chainalysis states that, "[a]ll of the CSAM data we analyze here is based on a subset of over 400 on-chain CSAM vendor wallets we've identified that were active between 2020 and 2023 and met a specific threshold of transaction activity. We observed over 10,000 wallets that sent funds to CSAM vendor wallets in 2023, which for the purposes of this analysis we label as CSAM buyers."[4]

In the years that Chainalysis has spent tracking these cryptocurrency wallets related to CSAM, the analysts have made important inferences that are helpful in investigations involving these wallets. Chainalysis analysts noticed patterns in which these criminals spent their money and noticed that many of those involved moved to instant exchangers in the years examined. These instant exchangers offer Monero, a privacy coin, and it is possible that this is why many of these illicit actors made this move. Another important inference that Chainalysis analysts have made is that many CSAM vendors have exposure to dark net markets and fraud shops. This is a helpful insight for financial crimes and law enforcement investigations, as this exposure can help draw conclusions, and raise the monetary value of cases that might ordinarily be low in instances involving CSAM.

The use of the 314b process is also extremely important in these situations. Many of the major cryptocurrency exchanges in the United States participate in this program, and they are able to provide information that can be helpful when piecing together investigations. This avenue of investigations relies on the quality of the KYC programs at these institutions. As money services businesses, these exchanges operating in the United States are required to have robust AML compliance programs, which includes a strong KYC program. As a result, this process is becoming more reliable for financial institutions to be able to gain insight to on-chain information, and to then use the tools at their discretion to detect activity of concern. Law enforcement is able to follow similar leads involving these major exchanges through the use of their subpoena power.

Financial Institutions can also rely on other known red flags to identify buyers and sellers of CSAM. These red flags include reviewing transactions for purchases that are related to this type of crime, such as certain computer hardware purchases and subscriptions to multiple VPN softwares. Identifying changes to VPN masking and infrastructure purchasing can reveal links to an individual's true identity that may even coincide with negative news pertaining to related crimes specifically involving an individual. The use of open-source data in this manner has always been critical to financial crimes investigations. Investigators should never overlook the power of this data in conjunction with transaction analysis to identify nefarious actors.

Despite efforts by Financial Institutions and cryptocurrency tracing companies to combat CSAM, this activity continues to be a growing issue online. One non-profit charitable organization, the Internet Watch Foundation ("IWF"), works to make the internet a safer place by identifying and removing CSAM from the internet. This organization produces an annual report detailing the trends and data observed for that year, based upon external reports through over 50 portals worldwide that are assessed by their Internet Content Analysts, and

based upon proactive analysis by the IWF team.[5] External reporting can come from the public, members of the organization, the hotline, police, and via other methods. In 2023, the IWF received 5% more reports of CSAM than was reported in 2022, for a total of 392, 665 reports.[6] Of these reports, 392,620 were reports of webpages and 45 reports of newsgroups. IWF defines newsgroups as, "Internet discussion groups dedicated to a variety of subjects. Users make posts to a newsgroup and others can see them and comment. Sometimes called 'Usenet', newsgroups were the original online forums and a precursor to the World Wide Web."[7] Of the webpages reported, 275,652 of them were confirmed to contain CSAM, which is an 8% increase from 2022. In addition, 6 newsgroups were confirmed to contain CSAM.

Another great non-profit working in this space is the National Center for Missing and Exploited Children ("NCMEC"). The mission of NCMEC is to "help find missing children, reduce child sexual exploitation, and prevent child victimization."[8] In 1998, in order to help combat online sexual exploitation of children, NCMEC created the CyberTipline. Those working for NCMEC may review the material reported via the tipline and then send it to law enforcement for further review. According to NCMEC's reporting, "the CyberTipline has received over 82 million reports and over 19,100 victims have been identified by law enforcement."[9] In addition to reviewing this material and reporting findings to law enforcement, "U.S. law enforcement [also] requires that U.S. based Electronic Service Providers ("ESPs") report instances of apparent child pornography that they become aware of on their systems to NCMEC's CyberTipline."[10] In turn, NCMEC also sends notices to these companies when there is suspected CSAM identified on the registered companies' servers.

A similar organization is the International Centre for Missing and Exploited Children ("ICMEC"). The organization has engaged assistance from several members of the financial industry to participate in a working group, called the ICMEC Cryptocurrency Working Group, which seeks to explore and provide information on the role of cryptocurrency in child sexual exploitation. This collaboration is crucial for gaining insight into the full picture of the issue, so that it can be tackled in a comprehensive manner and not from a siloed point of view. "ICMEC's Financial Coalitions Against Child Sexual Exploitation (FCACSEs) (U.S. and Asia Pacific) bring leaders in the financial and payments industries together to disrupt the economics of commercial child sexual exploitation and prevent the misuse of financial services technologies and platforms."[11] These efforts have had great success over the years. For instance, "[a]s a result of the combined efforts of Coalition partners and law enforcement, the use of credit cards to purchase child sexual exploitation material (CSEM) online has been virtually eliminated globally and websites offering CSEM have had to find alternative payment schemes for their illicit businesses."[12] These alternative schemes include moving to cryptocurrency, which is why

the ICMEC has pivoted to create new working groups and to work with law enforcement in this ever changing environment, in order to keep all children safe.

Despite the devotion of several organizations, law enforcement, private companies and financial institutions, the fight against CSAM still experiences some setbacks. While CSAM is a major issue, it at times is not the main focus, or can go under the radar of large AML and Financial Crimes divisions as the payments involved in the activity are so low. It takes a trained eye to recognize the patterns affiliated with this typology. It may also take someone with strong blockchain analysis skills and understanding, to trace the funds through wallets associated with this type of behavior, to ultimately trace the funds off ramp to fiat currency. There is a specific range of costs involved with the buying and selling of this material, but this is something you almost only see on the blockchain and something that only someone with knowledge on the typology would know. It is easy to focus on the multimillion-dollar cases splashed across the headlines of the news, but sometimes cases with lower dollar amounts, such as these CSAM related cases can help save so many lives of children globally.

Human Trafficking

Digital assets are also widely used to perpetrate human trafficking crimes. One particular instance where human trafficking and the use of digital assets frequently coincide is a fairly new form of cybercrime referred to as pig butchering. "[Pig butchering scams] – mostly run out of Southeast Asia - are given that name because they involve "fattening up" victims before taking everything they have. The con artists behind them take on false online identities and spend months financially grooming their victims to get them to invest on fraudulent cryptocurrency websites."[13] These scams can take many forms such as romance scams or investment scams, and usually always end in the victim sending cryptocurrency in large sums, which they will never see a return on investment. According to the FBI's 2023 Internet Crime Report, "in 2023, the losses reported due to Investment scams became the most of any crime type tracked by the IC3. Investment fraud losses rose from $3.31 billion in 2022 to $4.57 billion in 2023, a 38% increase. Within these numbers, investment fraud with a reference to cryptocurrency rose from $2.57 billion in 2022 to $3.94 billion in 2023, an increase of 53%."[14]

Human trafficking comes into play in these scams because large crime conglomerates are trafficking people from mostly Southeast Asia to perpetrate these scams. Most people have received that text message, starting mid-sentence, provoking conversation, but which happens to be from a wrong number. This is a tactic used by these pig butchering rings to hook the person on the other side of the line to engage, and hopefully continue to engage, until the scammer eventually gains the trust of the victim, and is able to convince the victim to send

funds, either fiat or cryptocurrency. But who is sending those text messages? Reporting conducted by both the New York Times and Chainalysis have revealed that "… individuals throughout China and Southeast Asia have been kidnapped, trafficked, and forced to work in labor camps housed within large compounds, carrying out pig butchering scams. Cities like Myawaddy in Myanmar are hot spots for this activity, as political instability there has allowed pig butchering gangs to operate with impunity."[15]

One of the biggest and well-known compounds, where these pig butchering gangs are housing victims, is a place in Myanmar called KK Park.[16] "KK Park is one of the biggest, most notorious romance scam compounds in operation today. Located in the… Myanmarese town of Myawaddy, KK Park is reported to hold over 2,000 trafficked romance scam workers."[17] These scam workers find themselves initially traveling abroad to pursue promises of high-paying jobs. However, once they arrive in their new country, they are kidnapped and brought to these compounds and are forced to scam. These victims are tortured and abused if they do not agree to participate.[18] These compounds are guarded, preventing the workers from leaving. Those in charge of these facilities are Chinese Gang organizations profiting off the scams, and also profiting from ransom payments that they solicit from the families of the trafficked scammers, and direct to be sent to cryptocurrency wallets. Some of these wallets have been identified by law enforcement. The sad reality is that this is an instance where we see "victims victimizing victims, and the only winners are Chinese Gangsters."[19] Therefore, combatting this issue is multifaceted, as national and local law enforcement is trying to protect victim citizens from losing their life savings to scams, while organizations, such as the International Justice Movement ("IJM") are working to stop the humanitarian crisis that has arisen as a result of the human trafficking taking place. [20]

Public private partnerships are essential to understanding how these pig butchering gangs work and how their activities can be disrupted. Financial institutions, private companies such as blockchain forensic companies, and law enforcement are all pivotal pieces to the solution. Financial institutions can monitor transaction flows through their institutions to identify certain entities and exchanges associated with these scams. As part of their compliance obligations, these financial institutions are then required to report this information to law enforcement for review and can help direct law enforcement to some of the most egregious activity flowing through American Banks. Private companies such as Chainalysis, are able to provide invaluable information concerning the identification of wallets involved in accepting scam fees from big butchering, as well as ransom payments from the families of the trafficked victims.

Financial institutions have had success in identifying entities tied to pig butchering gangs by reviewing wire transactions. The banks are alerted to fraud affecting their customers, and usually when the fraud is serious, in which large amounts of money were transferred and lost, or the fraud is identified as a scam, the cases are referred for further review to a team that completes more complex investigations. These teams are able to review the outgoing payments, which are usually sent via wire. The wires are reviewed to identify entities associated with the activity, and secondary wires are reviewed to identify further associated entities. This information can then be passed on to law enforcement through the proper escalation channels, so that they can investigate. Furthermore, if financial institutions see that funds have been sent on-chain, they can use the information request channels available, such as the 314b process, to obtain on-chain information and then use tools available to them to try to decipher the ultimate destination of funds.

Disrupting the activities of these pig butchering gangs is an essential piece to slowing the human trafficking that is occurring to promote their scam activities. Hopefully, with the helps of these public private partnerships, law enforcement can make arrests and hold the criminals perpetrating these crimes accountable. There have been some successful efforts to disrupt this activity. For instance, in 2023, "OKX [exchange]…collaborated with the United States Department of Justice in an investigation that led to Tether freezing approximately $225 million in USDT tokens linked to an international human trafficking syndicate in Southeast Asia responsible for romance scams."[21] There was also an operation in 2023 where South Korea-led Interpol "arrest[ed] 3,500 cybercriminals associated with online scamming and seize $300 million in funds, $100 million of which was made up of digital assets."[22]

Recent Rulings in Digital Asset Cases and The Changing Legal Landscape in Cases Involving Cryptocurrencies

Overall Rulings and Key Cases

A key case ruling that emerged this year was the finding of Roman Sterlingov being guilty of operating the bitcoin money laundering service Bitcoin Fog. This case marked a significant turning point into the inclusion of blockchain analytic tools in court cases. Specifically, Chainalysis and their proprietary tracing tool Reactor were directly used to illustrate the flow of funds and illicit activity that Bitcoin Fog was the center of. It also sparked what was seen as one of the first, hugely publicized differences in blockchain heuristics with another blockchain analysis tool, CipherTrace, showing a difference in results than Reactor. CipherTrace initially stated that Chainalysis's findings were inaccurate. However, they later had to redact that statement and instead stated their initial findings were inaccurate due to

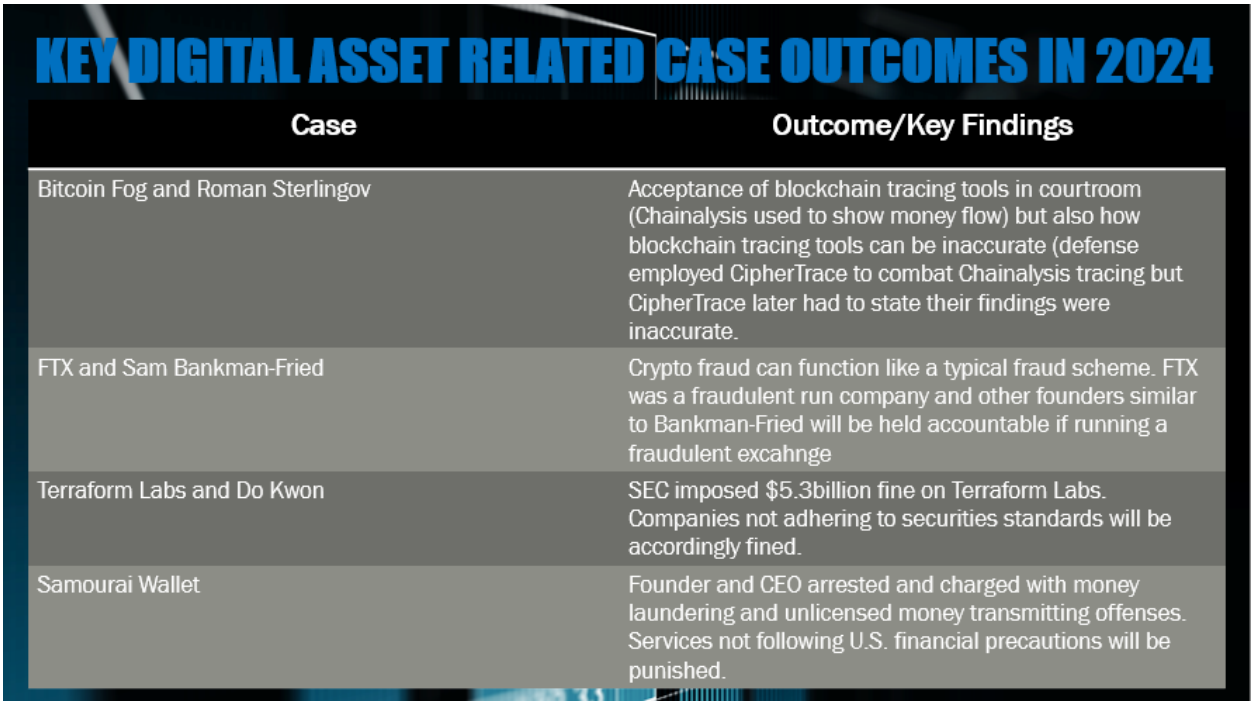
incorrect heuristics and attribution by their own proprietary blockchain tracing tool. The prosecution built their case on information from Chainalysis however the prosecution focused on the validity of that data. The defense commissioned a report by CipherTrace which had conflicting blockchain heuristics from Chainalysis. The Daubert hearing related to the Bitcoin Fog case saw the court decisively affirm the admissibility of Chainalysis blockchain analytics as evidence. CipherTrace later had to pull their report deeming the data as unverifiable and problems in data collection practices.[12]

It's long been debated whether these 3rd party tracing softwares and attribution services could be held up in court due to the possibility of inaccurate attribution. The Bitcoin Fog case serves as a great example of the acceptable use of outside blockchain heuristics being held up in court but also the inaccuracy outside blockchain heuristics can impose. It is always going to be crucial for investigating parties to back up the results of blockchain tracing software with direct open-source tracing, information from open-source tracing websites, and their own visualization of blockchain data.

The sentencing of Sam Bankman-Fried provides a good contrast case because the cryptocurrency tracing component wasn't key in his finding of guilt. FTX more so operated as a fraudulent crypto exchange that inflated its true holdings and stole billions of dollars from customers. This case was more representative of a traditional fraud scheme then the service being a vessel for illicit activity, though there has been illicit activity attributed to the exchange. Another critical case that emerged in the digital asset space was the SEC proposing a fine of $5.3 billion against Terraform Labs and its founder, Do Kwon. This came after the downfall of its algorithmic stablecoin which had large ripple effects across the entire cryptocurrency industry. U.S. based users were barred from accessing certain products. However, despite going through these legal challenges and the collapse of its stablecoin, Terraform continues to operate and offer certain products. [345]

Federal prosecutors charged Keonne Rodriguez and William Lonergan Hill, founders of Samourai Wallet, with conspiracy to commit money laundering. The charges relate to their operation of a cryptocurrency mixer that facilitated over $100 million in illegal transactions from dark web markets. Overall, Samourai facilitated around $2 billion in unlawful transactions between 2015 and the present. Rodriguez and Hill collected about $4.5 million in fees for their services. Rodriguez was arrested in Pennsylvania and Hill in Portugal, with the latter facing extradition to the U.S. Both face charges of conspiracy to commit money laundering and operating an unlicensed money transmitting business, carrying maximum sentences of 20 and 5 years, respectively. The U.S. government seized the Samourai Wallet website and its mobile application. The DOJ's press release indicates that Rodriguez and Hill openly encouraged users to launder criminal proceeds and targeted dark market participants in their marketing efforts.

This case follows other prosecutions of crypto mixing service operators, highlighting the U.S. government's ongoing crackdown on tools used to obscure illegal transactions.[67]



KEY DIGITAL ASSET RELATED CASE OUTCOMES IN 2024

Case	Outcome/Key Findings
Bitcoin Fog and Roman Sterlingov	Acceptance of blockchain tracing tools in courtroom (Chainalysis used to show money flow) but also how blockchain tracing tools can be inaccurate (defense employed CipherTrace to combat Chainalysis tracing but CipherTrace later had to state their findings were inaccurate.
FTX and Sam Bankman-Fried	Crypto fraud can function like a typical fraud scheme. FTX was a fraudulent run company and other founders similar to Bankman-Fried will be held accountable if running a fraudulent excahnge
Terraform Labs and Do Kwon	SEC imposed $5.3billion fine on Terraform Labs. Companies not adhering to securities standards will be accordingly fined.
Samourai Wallet	Founder and CEO arrested and charged with money laundering and unlicensed money transmitting offenses. Services not following U.S. financial precautions will be punished.

SEC Rulings

The SEC has enforced many rulings related to digital assets over the past year that are notable and are one of the major U.S. entities establishing precedent to go after cryptocurrency based fraudulent activity. Some examples of major cases include the following:

1. **SEC v. Geosyn Mining, LLC, et al.:** The Securities and Exchange Commission (SEC) filed charges against Geosyn Mining, LLC, a Texas-based crypto asset mining and hosting company, and its co-founders, Caleb Ward and Jeremy McNutt. They were accused of engaging in an unregistered and fraudulent securities offering on April 24, 2024.[1]

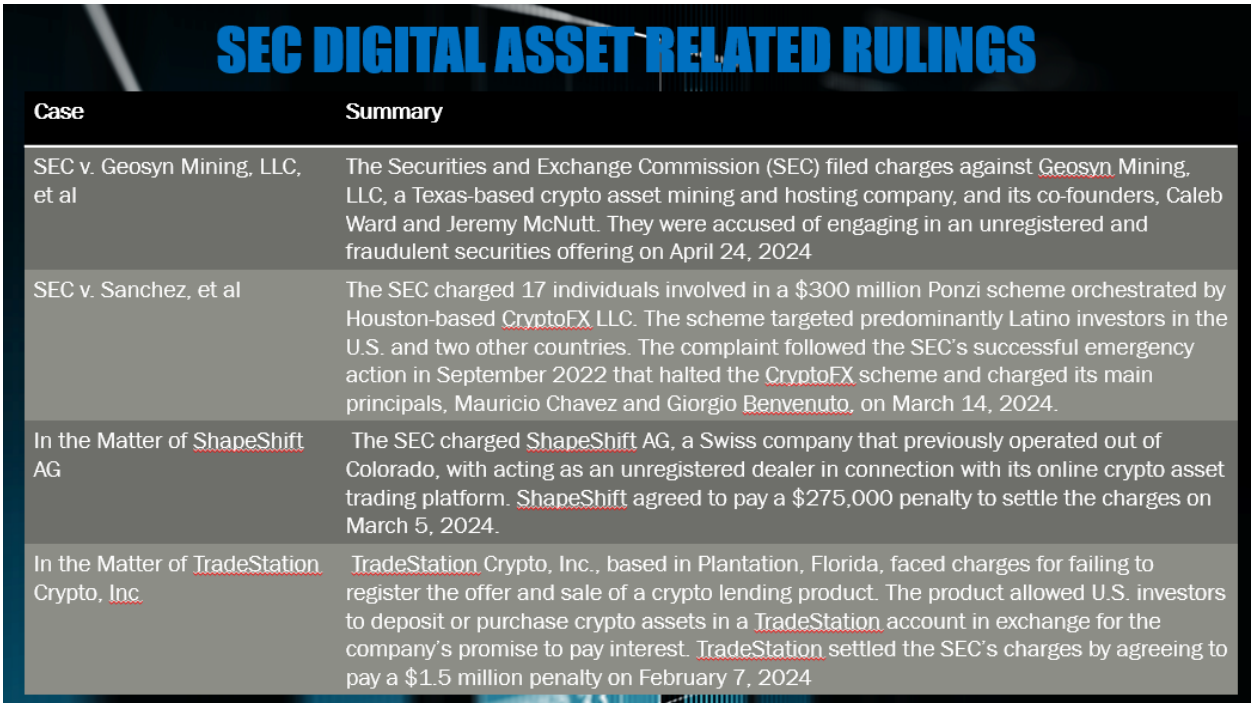
2. **SEC v. Sanchez, et al.:** The SEC charged 17 individuals involved in a $300 million Ponzi scheme orchestrated by Houston-based CryptoFX LLC. The scheme targeted predominantly Latino investors in the U.S. and two other countries. The complaint followed the SEC's successful emergency action in September 2022 that halted the CryptoFX scheme and charged its main principals, Mauricio Chavez and Giorgio Benvenuto, on March 14, 2024.[2]

3. **In the Matter of ShapeShift AG:** The SEC charged ShapeShift AG, a Swiss company that previously operated out of Colorado, with acting as an unregistered dealer in connection with its online crypto asset trading platform. ShapeShift agreed to pay a $275,000 penalty to settle the charges on March 5, 2024.[3]

4. **In the Matter of TradeStation Crypto, Inc.:** TradeStation Crypto, Inc., based in Plantation, Florida, faced charges for failing to register the offer and sale of a crypto lending product. The product allowed U.S. investors to deposit or purchase crypto assets in a TradeStation account in exchange for the company's promise to pay interest. TradeStation settled the SEC's charges by agreeing to pay a $1.5 million penalty on February 7, 2024.[4]

5. **SEC v. Sewell and Rockwell Capital Management LLC:** Brian Sewell and his company, Rockwell Capital Management, settled fraud charges related to a scheme targeting students taking Sewell's online crypto trading course known as the American Bitcoin Academy. The fraudulent scheme cost 15 students $1.2 million, as announced by the SEC on February 2, 2024.[5]

6. **SEC v. Lee, et al.:** Xue Lee (aka Sam Lee) and Brenda Chunga (aka Bitcoin Beautee) faced charges for their involvement in a fraudulent crypto asset pyramid scheme called HyperFund. The scheme raised more than $1.7 billion from investors worldwide, as reported on January 29, 2024.[6]



Future Regulations, Forecast, and Areas for Future Study - Collectively

Future Regulations: Regulatory bodies are expected to enforce stricter requirements for financial institutions, including more rigorous customer background checks, enhanced Know Your Customer (KYC) and Anti-Money Laundering (AML) processes, and more comprehensive transaction reporting. There is also a push for greater international cooperation to combat cross-border cryptocurrency-related crimes.

Regulations may specifically target decentralized finance (DeFi) platforms, requiring them to obtain licenses and implement risk mitigation measures.

The development and use of regulatory technology (RegTech) solutions are anticipated to play a significant role in monitoring transactions and ensuring compliance. Efforts may also be made to establish uniform regulatory frameworks across jurisdictions, provide legal recognition to smart contracts, and address the challenges posed by privacy-focused cryptocurrencies.

Forecast: The use of cryptocurrencies is expected to continue growing, both in legitimate commerce and illicit activities. Advancements in tracking technologies, such as blockchain analysis tools, will enhance the ability to trace and identify suspicious transactions.

Regulatory frameworks are forecasted to evolve rapidly, with updates to AML and CFT frameworks, the emergence of regulations for non-fungible tokens (NFTs) and stablecoins, and increased public-private partnerships to combat financial crimes.

There is also an anticipated need for greater education and awareness among consumers and businesses about the risks associated with cryptocurrencies and how to engage with them safely.

Areas for Future Study: Key areas for future research include the effectiveness of current regulations, the impact of technological advancements on illicit activities, regulatory gaps, the role of digital identities in enhancing KYC processes, the development of cybersecurity measures, and the influence of consumer awareness on preventing financial crimes. Researchers should also explore the economic impact of illicit activities, the development of forensic tools, behavioral analysis of individuals involved in financial crimes, international law enforcement collaboration, and the balance between privacy and transparency in financial transactions.

Additionally, the impact of artificial intelligence and machine learning on both facilitating and combating illicit activities, as well as the social and ethical considerations of

increased surveillance and data collection, are important areas for future study. This comprehensive overview highlights the evolving landscape of regulations, forecasts, and research priorities in the ongoing effort to combat illicit activities utilizing financial technologies and cryptocurrencies.

Throughout the past 3 years we've seen a huge increase in both public and private collaboration. Operation Shamrock was launched in April 2024 by Erin West, Deputy District Attorney of the Santa Clara District Attorney's Office, which appears to be the largest organized effort to date in the U.S. compromising both private and public participants to combat illicit activity in the digital currency space. Although illicit activity in the space is increasing and there appears to be a greater number of Americans falling victim to cryptocurrency related scams, there is now a clear organized effort to make a greater impact in both preventing these scams and dismantling the groups responsible for these scams.

More uniform information sharing has to be performed across both the private and public industries. Differences in information sharing among multiple financial institutions and multiple private companies is especially hindering responding to crypto scams and related crimes effectively. As investigators in both the public and private sector become more adjusted to investigating digital asset related crime and pooling resources, greater success will be seen.

Analytic Dissemination Plan

The following is a list federal agencies, private entities, and non-profits that stand to benefit from our research that stand to benefit from our research:

Securities and Exchange Commission

Cybersecurity & Infrastructure Agency

Financial Crimes Enforcement Network

Federal Bureau of Investigation

United States Secret Service

United States Postal Inspection Service

Homeland Security Investigations

Drug Enforcement Administration

Internal Revenue Service (Criminal Investigative Division)

U.S. Federal Reserve System

Office of the Comptroller of Currency

Office of the Director of National Intelligence and all associated IC partners

National Center for Missing and Exploited Children

International Center for Missing and Exploited Children

Evolve Bank & Trust

Citibank

Quad City Bank & Trust

Endnotes

Central Bank Digital Currencies & the Implications of Issuing CBDCs

1. Pros and Cons of Central Bank Digital Currency - 101 Blockchains
2. Fed outlines pros and cons of a US 'digital dollar' -- but avoids taking a stand (for now) (cnet.com)
3. Top 10 Advantages and Disadvantages of Central Bank Digital Currencies (CBDC) | NTT DATA Payment Service
4. Advantages of Central Bank Digital Currencies (CBDCs) (101blockchains.com)
5. The Fed - Security ConsiTop 10 Advantages and Disadvantages of Central Bank Digital Currencies (CBDC) | NTT DATA Payment Servicederations for a Central Bank Digital Currency (federalreserve.gov)
6. Money laundering and the privacy design of central bank digital currency - ScienceDirect
7. The Fed - Frequently Asked Questions (federalreserve.gov)
8. Establishing a US central bank digital currency: The right time or too risky? - Harvard Law School | Harvard Law School

Effects of AI on Digital Asset Related Crimes and Cyber Financial Crimes

1. https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/?sh=6c8bcc6d162b
2. https://cybermagazine.com/articles/cybercriminals-are-creating-a-darker-side-to-ai)
3. https://www.csoonline.com/article/1307021/will-generative-ai-kill-kyc-authentication.html
4. https://www.paymentvillage.org/blog/how-i-used-deepfakes-to-bypass-security-verifications-in-a-bank
5. https://www.thistleinitiatives.co.uk/blog/ai-generated-id-documents-bypassing-well-known-kyc-software
6. https://www.csoonline.com/article/1307021/will-generative-ai-kill-kyc-authentication.html
7. https://cybermagazine.com/articles/cybercriminals-are-creating-a-darker-side-to-ai
8. https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/?sh=6c8bcc6d162b
9. https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/?sh=6c8bcc6d162b

How have the improvements in AI enhanced crimes of spoofing, phishing, and impersonation in Digital Asset Crime and Cyber-Financial Crime

1. https://www.cnbc.com/2023/06/08/ai-is-helping-hackers-make-better-phishing-emails.html
2.https://www.forbes.com/sites/emilsayegh/2023/04/11/almost-human-the-threat-of-ai-powered-phishing-attacks
3.https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams
4..https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice
5.https://www.forbes.com/sites/cyrusfarivar/2023/04/20/alleged-crypto-scammers-used-ai-and-actors-as-faux-ceo
6.. https://www.kktv.com/2024/07/17/ftc-warns-government-impersonation-scams/

Is There a Path Forward?

1.https://sites.lsa.umich.edu/mje/2024/02/14/the-dark-alliance-addressing-the-rise-of-ai-financial-frauds-and-cyber-scams/#:~:text=There

2.https://bankingjournal.aba.com/2024/02/generative-artificial-intelligence-threat-and-solution-or-financial-crime/
3. https://fintechmagazine.com/fraud-id-verification/complyadvantage-state-of-financial-crime-2024
4. https://diro.io/artificial-intelligence-to-fight-financial-fraud/
5.https://techcrunch.com/sponsor/nvidia-aws/financial-fraud-is-evolving-faster-than-ever-but-ai-is-helping-fintechs-fight-back/

6.https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams
7.https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustwort hy-development-and-use-of-artificial-intelligence/
8.https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
9..https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
10. https://www.csg.org/2023/12/06/artificial-intelligence-in-the-states-emerging-legislation/
11. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states
12. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states

Zero Knowledge Proofs and How They Can Correlate with Illicit Activity

1. https://decrypt.co/resources/zero-knowledge-proofs-explained-learn-guide
2.https://blog.spheron.network/how-zero-knowledge-proofs-are-changing-the-future-of-privacy-and-security
3. https://chain.link/education-hub/zero-knowledge-proof-use-cases
4. https://blockgeeks.com/guides/zero-knowledge-proofs/
5. https://www.wilsoncenter.org/article/dont-trust-when-you-can-verify-primer-zero-knowledge-proofs

Current Trends in the Digital Asset Space

1. The Chainalysis 2024 Crypto Crime Report
2. The Chainalysis 2024 Crypto Crime Report
3. What Is Human Trafficking? | Homeland Security (dhs.gov)
4. The Chainalysis 2024 Crypto Crime Report
5. Online Child Sexual Abuse Reports Analysis | IWF 2023 Annual Report
6. Online Child Sexual Abuse Reports Analysis | IWF 2023 Annual Report
7. Online Child Sexual Abuse Reports Analysis | IWF 2023 Annual Report
8. About Us (missingkids.org)
9. Child Sexual Abuse Material (missingkids.org)
10. Child Sexual Abuse Material (missingkids.org)
11. Microsoft Word - Cryptocurrency 03.10.21.docx (icmec.org)
12. Microsoft Word - Cryptocurrency 03.10.21.docx (icmec.org)
13. https://www.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html#:~:text=The%20scams%20%E2%80%93%20mostly%20run%20out,invest%20on%20fraudulent%20cryptocurrency%20websites.
14. ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf?trk=public_post_comment-text
15. https://chainalysis.com/blog/pig-butchering-human-trafficking/
16. https://chainalysis.com/blog/pig-butchering-human-trafficking/
17. https://chainalysis.com/blog/pig-butchering-human-trafficking/
18. $75 Billion Lost to Pig-Butchering Scam, New Study Estimates | TIME

19. https://www.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html#:~:text=The%20scams%20%E2%80%93%20mostly%20run%20out,invest%20on%20fraudulent%20cryptocurrency%20websites.
20. https://www.chainalysis.com/blog/pig-butchering-human-trafficking/
21. https://www.chainalysis.com/blog/pig-butchering-human-trafficking/
22. https://www.chainalysis.com/blog/pig-butchering-human-trafficking/

Recent Rulings in Digital Asset Cases and the Changing Legal Landscape in Cases Involving Cryptocurrencies

1. https://www.justice.gov/usao-dc/pr/jury-finds-russian-swedish-operator-bitcoin-fog-guilty-running-darknet-cryptocurrency
2. https://fortune.com/crypto/2024/03/13/mastercard-ciphertrace-blockchain-analytics-chainalysis-bitcoin-fog/
3. https://www.nytimes.com/2024/03/28/technology/sam-bankman-fried-sentenced.html
4. https://www.reuters.com/legal/terraform-labs-make-final-pitch-jury-civil-fraud-trial-wraps-2024-04-05/#:~:text=A%20jury%20in%20Manhattan%20found%20Singapore-based%20Terraform%20Labs,before%20their%20stablecoin%27s%202022%20collapse%20shocked%20cryptocurrency%20markets.
5. https://www.coindesk.com/policy/2024/04/05/new-york-jury-finds-do-kwon-terraform-labs-liable-for-fraud-in-sec-case/
6. https://www.coindesk.com/policy/2024/04/24/samourai-wallet-founders-arrested-and-charged-with-money-laundering/
7. https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering
8. SEC.gov | Geosyn Mining, LLC, Caleb Joseph Ward, and Jeremy George McNutt
9. SEC.gov | Ismael Zarco Sanchez, et al.
10. SEC.gov | On Today's Episode of As the Crypto World Turns: Statement on ShapeShift AG
11. SEC.gov | SEC Charges TradeStation Crypto for Unregistered Offer and Sale of Crypto Asset Lending Product
12. SEC.gov | Brian Sewell and Rockwell Capital Management LLC
13. SEC.gov | SEC v. Lee et al. Civil Action No. 3:23-cv-125-OAW (D. Conn.)

Citations Separated by Section

Citations for Central Bank Digital Currencies & the Implications of Issuing CBDCs

(U) | 101 Blockhains | Feb. 2021 | Pros and Cons of Central Bank Digital Currency | https://101blockchains.com/central-bank-digital-currency-pros-and-cons/

(U) | CNET | Jan. 2022 | Fed outlines the pros and cons of a US "digital dollar" but avoids taking a stand for now | https://www.cnet.com/personal-finance/crypto/central-bank-digital-currencies-everything-you-need-to-know/

(U) | NTT Data Payment Services | April 2024 | https://www.nttdatapay.com/blog/advantages-disadvantages-of-central-bank-digital-currencies

(U) | 101 Blockchains | July 2021 | https://101blockchains.com/advantages-of-central-bank-digital-currencies/

(U) | Federal Reserve | Feb. 2022 | https://www.federalreserve.gov/econres/notes/feds-notes/security-considerations-for-a-central-bank-digital-currency-20220203.html

(U) | Wang | Review of Economic Dynamics - Money laundering and the privacy design of central bank digital currency | Dec. 2023 | https://www.sciencedirect.com/science/article/abs/pii/S1094202523000236

(U) | Federal Reserve | April 2023 | Central Bank Digital Currency (CBDC) | https://www.federalreserve.gov/cbdc-faqs.htm

(U) | Harvard Law Today | Oct. 2022 | Establishing a US central bank digital currency: The right time or too risky? | https://hls.harvard.edu/today/establishing-a-us-central-bank-digital-currency-the-right-time-or-too-risky/

Citations for Effects of AI on Digital Asset Related Crime and Cyber-Financial Crimes

(U) | Forbes | June 2023 | AI And Cybercrime Unleash A New Era Of Menacing Threats | https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/?sh=6c8bcc6d162b

(U) | Cyber Magazine | October 2023 | Cybercriminals are creating a darker side to AI | https://cybermagazine.com/articles/cybercriminals-are-creating-a-darker-side-to-ai

(U) |CSO | Feb. 2024 | Will generative AI Kill KYC authentication? | https://www.csoonline.com/article/1307021/will-generative-ai-kill-kyc-authentication.html

(U) | Payment Village | How I used deepfakes to bypass security verifications in a bank | https://www.paymentvillage.org/blog/how-i-used-deepfakes-to-bypass-security-verifications-in-a-bank

(U) | Thistle Initiatives | March 2024 | AI-generated ID documents bypassing well-known KYC software | https://www.thistleinitiatives.co.uk/blog/ai-generated-id-documents-bypassing-well-known-kyc-software

How have the improvements in AI enhanced crimes of spoofing, phishing, and impersonation in Digital Asset Crime and Cyber-Financial Crime

(U) | CNBC | Jun. 2023 | A.I. is Helping Hackers Make Better Phishing Emails | https://www.cnbc.com/2023/06/08/ai-is-helping-hackers-make-better-phishing-emails.html

(U) | Forbes | Apr. 2023 | Almost Human: The Threat Of AI-Powered Phishing Attacks | https://www.forbes.com/sites/emilsayegh/2023/04/11/almost-human-the-threat-of-ai-powered-phishing-attacks/

(U) | Harvard Business Review | May 2024 | AI Will Increase the Quantity — and Quality — of Phishing Scams | https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

(U) | New Yorker | Mar. 2024 | The Terrifying A.I. Scam That Uses Your Loved One's Voice | https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice

(U) | Forbes | Apr. 2023 | Alleged Crypto Scammers Used AI And Actors as Faux CEOs| https://www.forbes.com/sites/cyrusfarivar/2023/04/20/alleged-crypto-scammers-used-ai-and-actors-as-faux-ceos/

(U) | 11 News| Jul. 2024 | FTC Warns of Government Impersonation Scams | https://www.kktv.com/2024/07/17/ftc-warns-government-impersonation-scams/

Citations for Is There a Path Forward?

(U) | Michigan Journal of Economics | Feb. 2024 | The Dark Alliance: Addressing the Rise of AI Financial Frauds and Cyber Scams| https://sites.lsa.umich.edu/mje/2024/02/14/the-dark-alliance-addressing-the-rise-of-ai-financial-frauds-and-cyber-scams/#:~:text=There

(U) | American Bar Association | Feb. 2024 | Generative artificial intelligence: Threat and Solution for Financial Crime?| https://bankingjournal.aba.com/2024/02/generative-artificial-intelligence-threat-and-solution-or-financial-crime/

(U) | Fintech Magazine | Jan. 2024 | How AI is Changing the Financial Crime Landscape| https://fintechmagazine.com/fraud-id-verification/complyadvantage-state-of-financial-crime-2024

(U) | Diro | May 2024 | Artificial Intelligence to Fight financial Fraud| https://diro.io/artificial-intelligence-to-fight-financial-fraud/

(U) | Techcrunch | accessed July 2024 | Financial fraud is Evolving Faster than Ever. But AI is Helping Fintechs Fight Back | https://techcrunch.com/sponsor/nvidia-aws/financial-fraud-is-evolving-faster-than-ever-but-ai-is-helping-fintechs-fight-back/

(U) | White House | Oct. 2023 | Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

(U) | European Parliament | Aug. 2023 | EU AI Act: First Regulation on Artificial Intelligence| https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

(U) | Council of State Governments | Dec. 2023 | Artificial Intelligence in the States: Emerging Legislation | https://www.csg.org/2023/12/06/artificial-intelligence-in-the-states-emerging-legislation/

(U) | White and Case | May 2024 | AI Watch: Global Regulatory Tracker - United States | https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states

(U) | Harvard Business Review | May 2024 | AI Will Increase the Quantity — and Quality — of Phishing Scams | https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

Citations for Zero Knowledge Proofs and How They Can Correlate with Illicit Activity

(U) | Decrypt | March 2020 | What Are Zero Knowledge Proofs? | https://decrypt.co/resources/zero-knowledge-proofs-explained-learn-guide

(U) | Spheron | Dec. 2023 | How Zero Knowledge Poofs Are Changing the Future of Privacy and Security | https://blog.spheron.network/how-zero-knowledge-proofs-are-changing-the-future-of-privacy-and-security

(U) | Chainlink | Nov. 2023 | Zero Knowledge Proof: Applications and Use Cases | https://chain.link/education-hub/zero-knowledge-proof-use-cases

(U) | Blockgeeks | Nov. 2023 | Demystifying Zero Knowledge Proofs: A Comprehensive Guide | https://blockgeeks.com/guides/zero-knowledge-proofs/

(U) | Wilson Center | Feb. 2024 | Don't Trust When You Can Verify: A Primer on Zero-Knowledge Proofs | https://www.wilsoncenter.org/article/dont-trust-when-you-can-verify-primer-zero-knowledge-proofs

Citations for Current Trends in the Digital Asset Space

(U) | Chainalysis | Feb. 2024 | The 2024 Crypto Crime Report | The Chainalysis 2024 Crypto Crime Report

(U) | DHS | Sept. 2022 | What is Human Trafficking | What Is Human Trafficking? | Homeland Security (dhs.gov)

(U) | IWF | 2023 | IWF 2023 Annual Report | Online Child Sexual Abuse Reports Analysis | IWF 2023 Annual Report

(U) | National Center for Missing & Exploited Children | About Us | About Us (missingkids.org)

(U) | National Center for Missing & Exploited Children | Child Sexual Abuse Material | Child Sexual Abuse Material (missingkids.org)

(U) | The International Centre for Missing & Exploited Children and Standard Chartered | Feb. 2021 | Cryptocurrency and the Trade of Online Child Sexual Abuse Material | Microsoft Word - Cryptocurrency 03.10.21.docx (icmec.org)

(U) | CNN | June 2024 | Killed by a scam: A father took his life after losing his savings to international criminal gangs. He's not the only one | https://www.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html

(U) |FBI | 2023 | 2023 Internet Crime Report | ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf?trk=public_post_comment-text

(U) | Chainalysis | Feb. 2024 | The On-chain Footprint of Southeast Asia's 'Pig Butchering' Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed | Pig Butchering Gangs, Human Trafficking, and Crypto: An Analysis (chainalysis.com)

(U) | TIME | Feb. 2024 | New Study Estimates as Much as $75 Billion in Global Victims' Losses to Pig-Butchering Scam | $75 Billion Lost to Pig-Butchering Scam, New Study Estimates | TIME

Citations for Recent Rulings in Digital Asset Cases and The Changing Legal Landscape in Cases Involving Cryptocurrencies

(U) | U.S. Dept. of Justice | March 2024 | Jury Finds Russian-Swedish Operator of 'Bitcoin Fog' Guilty of Running the Darknet Cryptocurrency Mixer | https://www.justice.gov/usao-dc/pr/jury-finds-russian-swedish-operator-bitcoin-fog-guilty-running-darknet-cryptocurrency

(U) | Fortune | March 2024 | Mastercard-owned CipherTrace tells clients it is shutting down key products | https://fortune.com/crypto/2024/03/13/mastercard-ciphertrace-blockchain-analytics-chainalysis-bitcoin-fog/

(U) | The New York Times | March 2024 | Sam Bankman-Fried Sentenced to 25 Years in Prison | https://www.nytimes.com/2024/03/28/technology/sam-bankman-fried-sentenced.html

(U) | Reuters | April 2024 | Terraform Labs and founder Do Kwon found liable in US civil fraud trial | Terraform Labs and founder Do Kwon found liable in US civil fraud trial | Reuters

(U) | CoinDesk | April 2024 | New York Jury Finds Do Kwon, Terraform Labs Liable for Fraud in SEC Case | https://www.coindesk.com/policy/2024/04/05/new-york-jury-finds-do-kwon-terraform-labs-liable-for-fraud-in-sec-case/

(U) | CoinDesk | April 2024 | Samourai Wallet Founders Arrested and Charged With Money Laundering | https://www.coindesk.com/policy/2024/04/24/samourai-wallet-founders-arrested-and-charged-with-money-laundering/

(U) | U.S. Dept. of Justice | April 2024 | Founders And CEO Of Cryptocurrency Mixing Service Arrested And Charged With Money Laundering And Unlicensed Money Transmitting Offenses | https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering

(U) | SEC | April 2024 | Geosyn Mining, LLC, Caleb Joseph Ward, and Jeremy George McNutt | SEC.gov | Geosyn Mining, LLC, Caleb Joseph Ward, and Jeremy George McNutt

(U) | SEC | March 2024 | Ismael Zarco Sanchez, et al. |SEC.gov | Ismael Zarco Sanchez, et al.

(U) | SEC | March 2024 | On Today's Episode of As the Crypto World Turns: Statement on ShapeShift AG | SEC.gov | On Today's Episode of As the Crypto World Turns: Statement on ShapeShift AG

(U) | SEC | Feb 2024 | SEC Charges TradeStation Crypto for Unregistered Offer and Sale of Crypto Asset Lending Product | SEC.gov | SEC Charges TradeStation Crypto for Unregistered Offer and Sale of Crypto Asset Lending Product

(U) | SEC | Feb 2024 | Brian Sewell and Rockwell Capital Management LLC |SEC.gov | Brian Sewell and Rockwell Capital Management LLC

(U) | SEC | Jan 2024 | SEC v. Lee et al. Civil Action No. 3:23-cv-125-OAW (D. Conn.) |SEC.gov | SEC v. Lee et al. Civil Action No. 3:23-cv-125-OAW (D. Conn.)

Appendi

Appendix A: Global Landscape of CBDCs