CFTC

COMMODITY FUTURES TRADING COMMISSION

Technology Advisory Committee Meeting – March 22, 2023

TAC Sponsor

Commissioner Christy Goldsmith Romero

CFTC

COMMODITY FUTURES TRADING COMMISSION

Opening Remarks

Commissioner
Christy Goldsmith Romero

Chairman
Rostin Behnam

Commissioner
Kristin N. Johnson

Commissioner
Summer K. Mersinger

Commissioner
Caroline D. Pham

CFTC

COMMODITY FUTURES TRADING COMMISSION

Topic 1: Exploring Issues in Decentralized Finance

METRIKA

Decentralization

March 22, 2023

Prepared for:

CFTC
COMMODITY FUTURES TRADING COMMISSION

CONFIDENTIAL

Decentralization is not new

- Decentralization has existed in history in so many forms, e.g. democracy, tax authorities, state-nations
- The least decentralized environment has historically been finance
- Today modern technology (cryptography, consensus mechanisms) eliminates all obstacles towards a “decentralized computer” for DeFi and Dapps
- Bringing decentralization to finance requires a true understanding of the means and goals of DeFi

Decentralization has many aspects

- **Definition**: *"Decentralization refers to the transfer of control and decision-making from a centralized entity (individual, organization, or group thereof) to a distributed network."*

- Protocol decentralization has commonly included the following dimensions:
  - Open Source (development of technology)
  - Network / Nodes (operations)
  - Custody (variety of options/wallets)
  - Dapps / DeFi (application logic)
  - Decision Making & Economy (governance & token economics)
- Ecosystem decentralization varies across its components
  - Multiple L2s, bridges, exchanges, oracles, etc. are part of the ecosystem

Benefits from “decentralization”

- Increases transparency and accountability
  - Could we have prevented “SVB problem” with decentralization?
- Enhances security
  - Could New Zealand Bank, Robinhood data breaches have been prevented through decentralization?
- Enables greater autonomy and control

Some key challenges to overcome

- Bootstrapping
  - Threshold levels needed
- Technological Maturity
  - Scalability
  - Interoperability
- Governance
  - “Tragedy of the Commons”
- Lack of risk management tools by traditional finance

Conclusion

- The benefits of decentralization far outweigh the challenges
- Some challenges will self-resolve as a function of time and technology progress
- New tools and practices for governance and risk management need to be applied to DeFi to allow broader adoption

METRIKA

TRM

DeFi Challenges and Opportunities

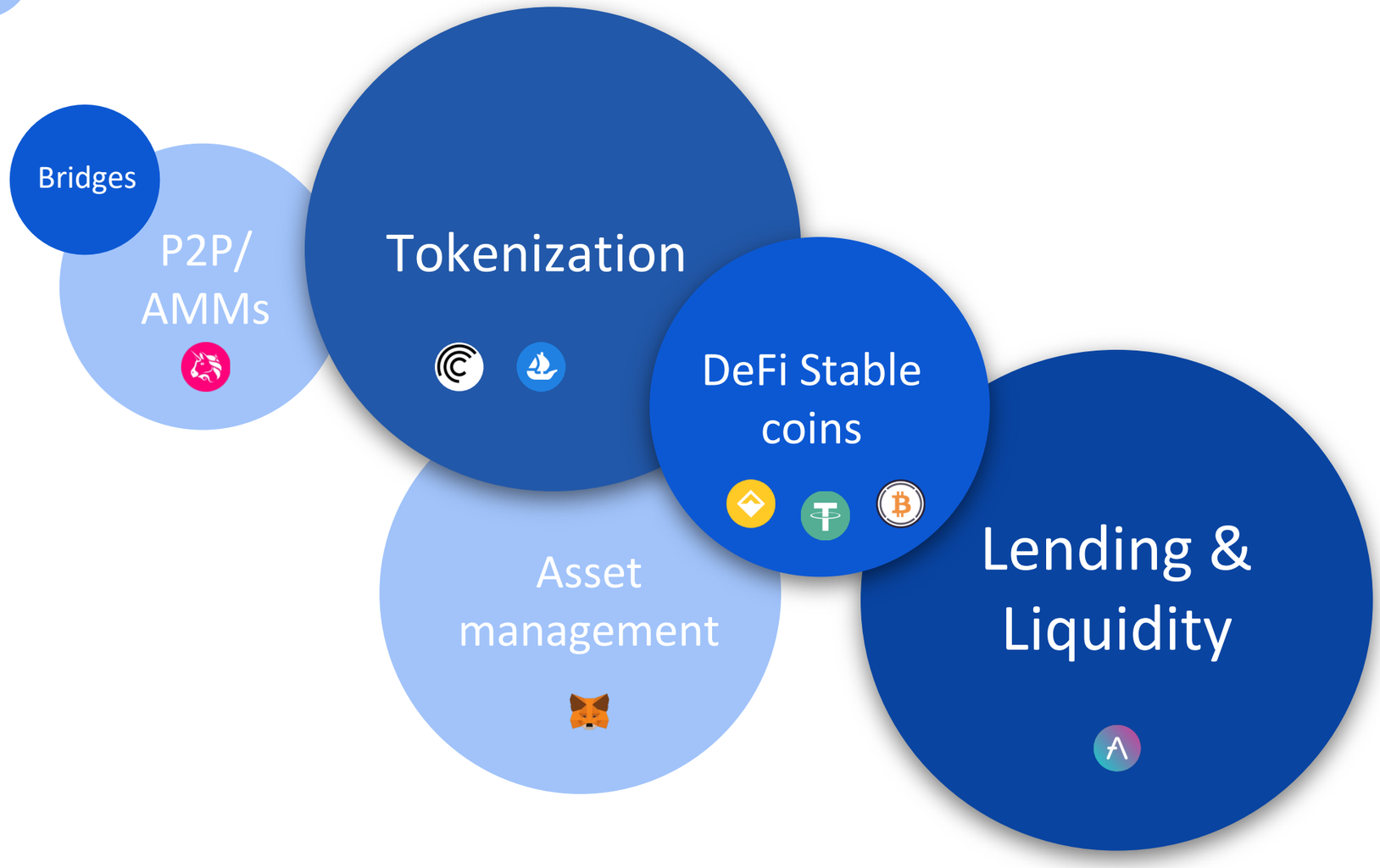
CFTC Technology Advisory Committee

March 22, 2023

TRMLABS.COM

2022 © All Rights Reserved. TRM Labs.

DeFi Enables



Why Do We Care?

https://defillama.com/

The total value locked (TVL) in DeFi has exploded in the past two years, from about $10 billion in October 2020 to $47 billion in February 2023. DeFi has been stress tested and did not fail.

What are the vulnerabilities we need to address?

Internal

Technology Risks (hacks)

- Code exploits
- Infrastructure attacks
- Protocol attacks

Frauds and scams

Sanctions

External

Market Manipulation

- Flash Loans
- Oracle manipulation

Money Laundering

- Cross chain hops
- Decentralized exchanges

Decentralized Finance

What are the vulnerabilities we need to address?

Internal | External

Technology Risks (hacks)

- Code exploits
- Infrastructure attacks
- Protocol attacks

Frauds and scams

Sanctions

Market Manipulation

- Flash Loans
- Oracle manipulation

Money Laundering

- Cross chain hops
- Decentralized exchanges

Technology Risks

- 2022 was record year for hacks
- $3.7 billion in stolen funds.
- 80% against DeFi

Target	Month	Amount Stolen	Type of Attack
Ronin Bridge	March	$612 million	Infrastructure Attack
BNB Chain	October	$570 million	Code Exploit
FTX	November	$400 million	Unknown
Wormhole	February	$326 million	Code Exploit
Nomad Bridge	August	$190 million	Code Exploit
Beanstalk	April	$182 million	Protocol Attack
Wintermute	April	$160 million	Infrastructure Attack
Maiar/Elrond	June	$113 million	Infrastructure Attack
Mango Markets	October	$112 million	Infrastructure Attack
Harmony Bridge	June	$100 million	Infrastructure Attack

TRM

© TRM Labs. All rights reserved.

What are the vulnerabilities we need to address?

Internal	External
Technology Risks (hacks) • Code exploits • Infrastructure attacks • Protocol attacks	Market Manipulation • Flash Loans • Oracle manipulation
Frauds and scams	Money Laundering • Cross chain hops • Decentralized exchanges
Sanctions	

How do we mitigate the risk of frauds and scams in the DeFi ecosystem?

11 “mega” investment fraud schemes received >$100m in 2022s

Between January and October 2022, TRM identified 11 “mega” fraud schemes, which each received more than $100M and together accounted for about 74% of the total amount.

Decentralized Finance

What are the vulnerabilities we need to address?

Internal

Technology Risks (hacks)

- Code exploits
- Infrastructure attacks
- Protocol attacks

Frauds and scams

Sanctions

External

Market Manipulation

- Flash Loans
- Oracle manipulation

Money Laundering

- Cross chain hops
- Decentralized exchanges

Sanctions Risk

How should we do sanctions compliance in the DeFi ecosystem?

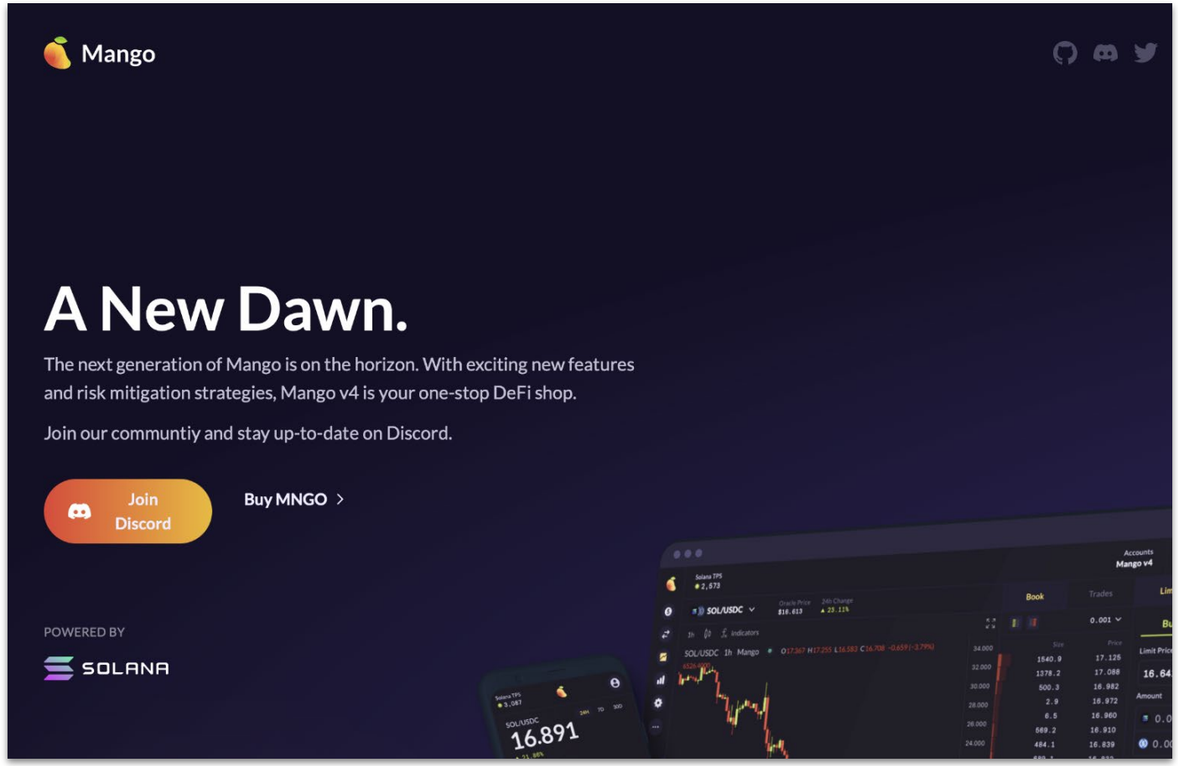
Decentralized Finance

What are the vulnerabilities we need to address?

Internal	External
Technology Risks (hacks) • Code exploits • Infrastructure attacks • Protocol attacks Frauds and scams Sanctions	Market Manipulation • Flash Loans • Oracle manipulation Money Laundering • Cross chain hops • Decentralized exchanges

Market Manipulation

- Mango Markets
- DeFi services
- Oracle Manipulation
- Deposit funds
- Long and short position
- Not illegal today . . .



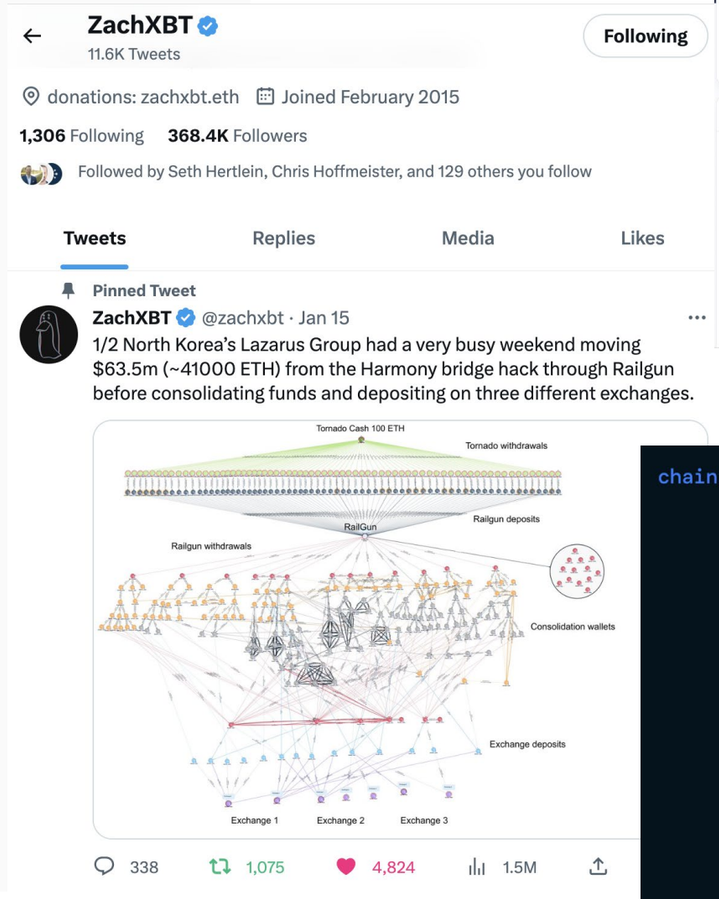
Decentralized Finance

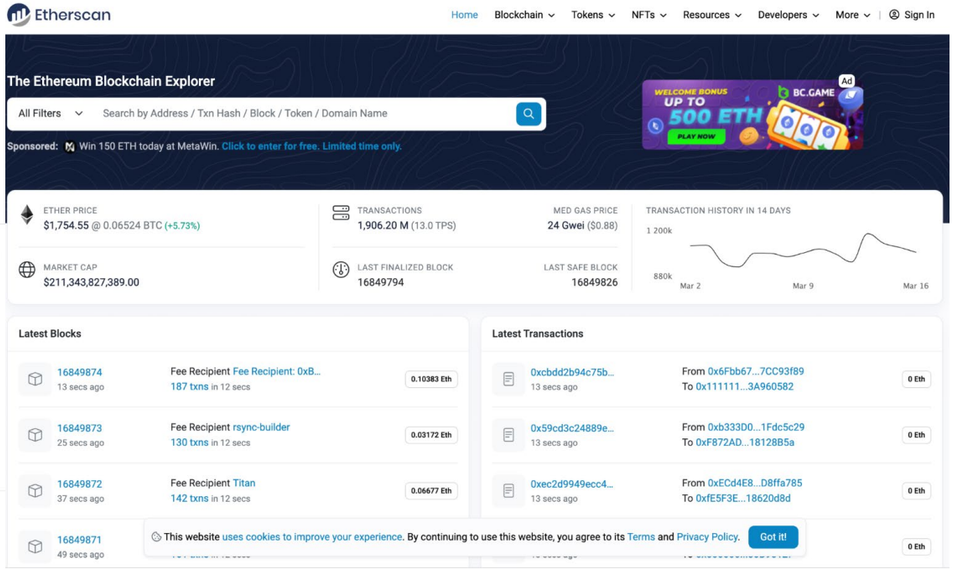
What are the vulnerabilities we need to address?

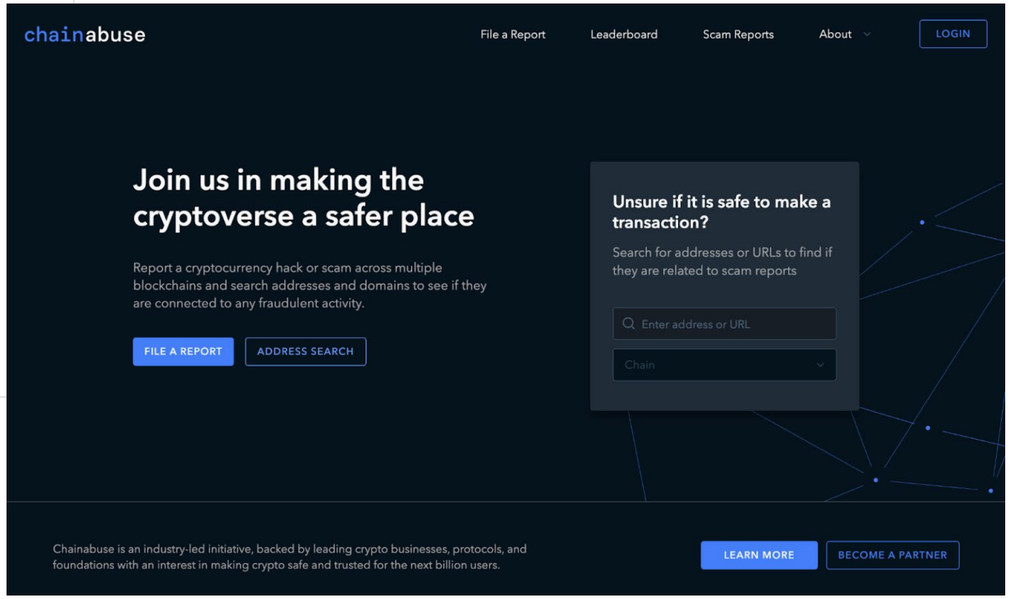
Internal	External
Technology Risks (hacks) • Code exploits • Infrastructure attacks • Protocol attacks	Market Manipulation • Flash Loans • Oracle manipulation
Frauds and scams	**Money Laundering** • Cross chain hops • Decentralized exchanges
Sanctions	

The promise of blockchain technology

Public







The promise of blockchain technology

Permanent

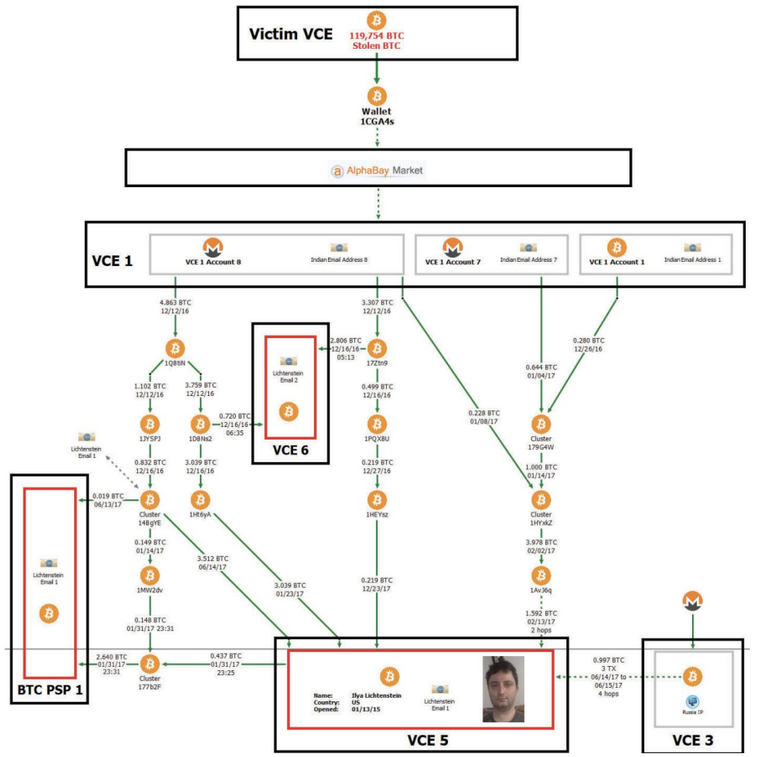
Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Tuesday, February 8, 2022

Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency

Government Seized $3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange



The promise of blockchain technology

Private

Privacy-Enhancing Technologies (PETs) like zero-knowledge proofs are being deployed at the protocol, middleware, and application layers to advance data protection and privacy goals. PETs can be used to make information on blockchains private, such as transaction details or data on blockchain-based computer programs.

While there are vulnerabilities, the technology can mitigate the risks.

Internal

Hacks

- Code exploits
- Infrastructure attacks
- Protocol attacks

Frauds and scams

Sanctions

External

Market Manipulation

- Flash Loans
- Oracle manipulation

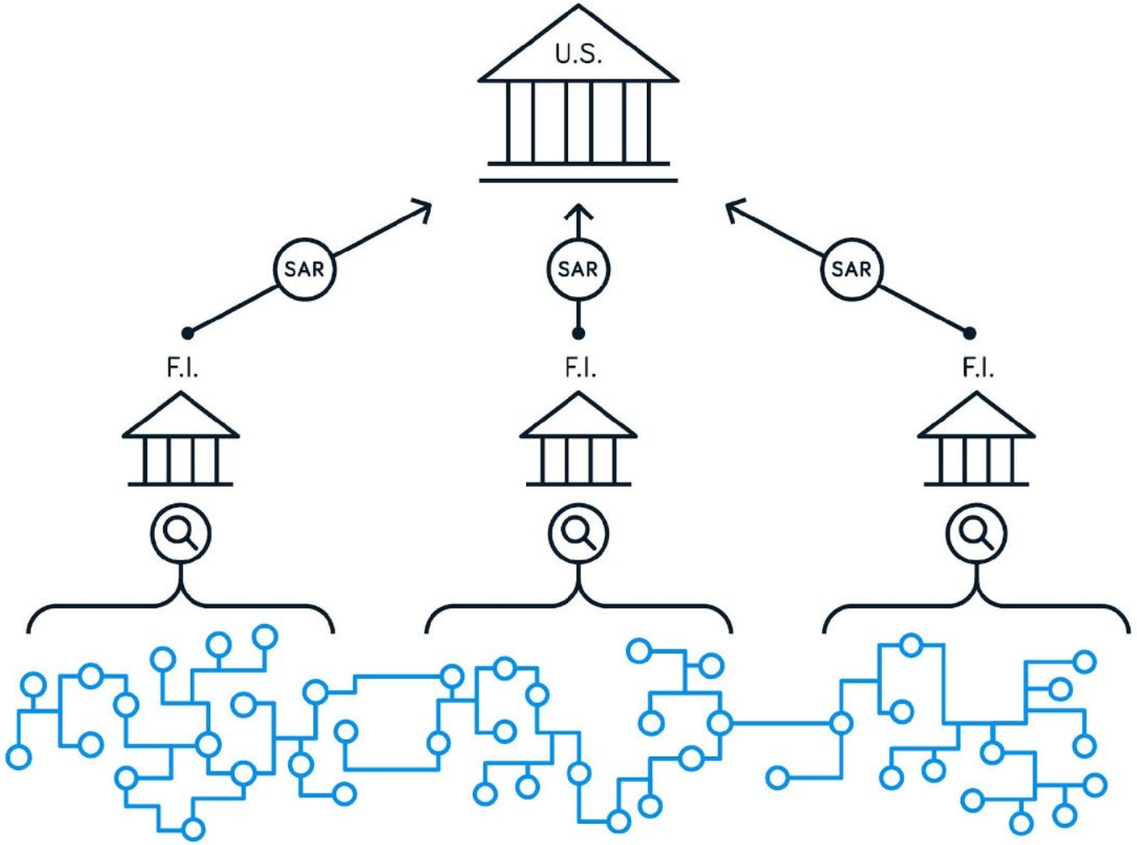
Money Laundering

- Cross chain hops
- Decentralized exchanges

Centralized VASPs remain critical to the off ramping of illicit funds - "All Roads Lead to VASPs."

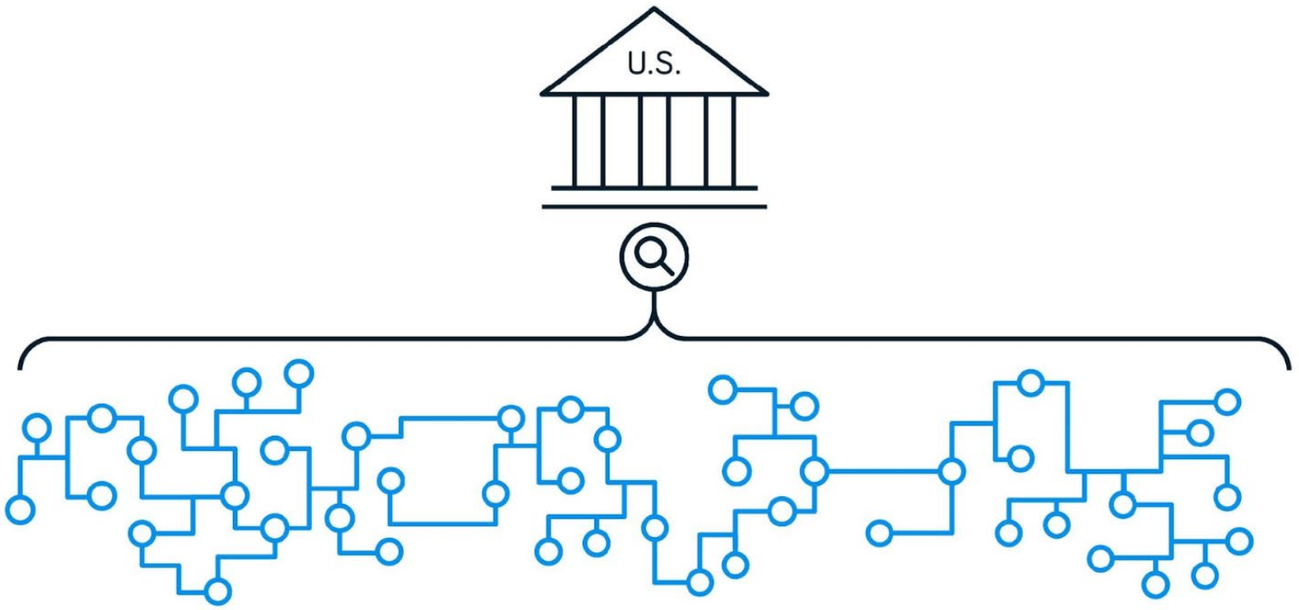
TODAY'S MODEL

Regulatory/Policy Landscape Today



FUTURE

Blockchains can change the face of regulation



DIGITAL IDENTITY, PRIVACY, UNHOSTED WALLETS: WHAT'S ON THE HORIZON?

JILL GUNTER

CAROLE HOUSE

COMMODITY FUTURES TRADING COMMISSION (CFTC) TECHNOLOGY ADVISORY COMMITTEE (TAC)

MARCH 2023

IDENTITY OVERVIEW - A COMPLEX ECOSYSTEM

What is Identity?

A unique representation of a person in a specific context

Ex.:

- **Official:** taxpayer, veteran
- **Social:** social media, gamer profile, reputation
- **Financial:** accountholder, credit applicant, ultimate beneficial owner

Attributes

Physical or behavioral characteristics by which an individual is uniquely recognizable

Ex.: Name, address, DOB, email, IP address, credit or gaming history

Evidence

Document or information provided to support the claimed identity

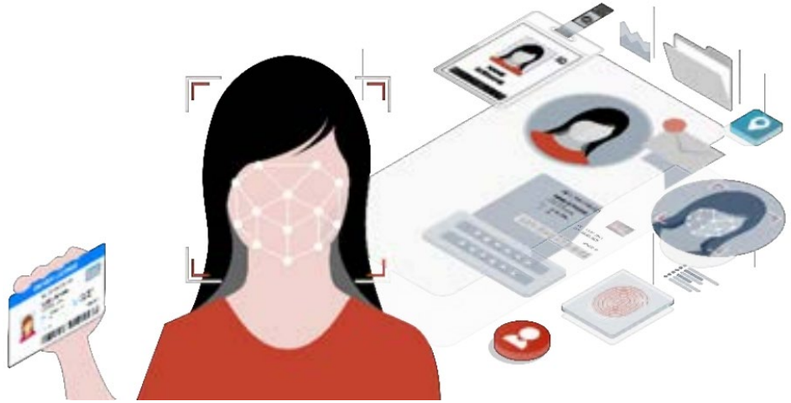
Ex.: driver's license, utility bill, selfie

Components of Identity Assurance

Categories for degree of confidence that the claimed identity is the person's real identity

- Identity Proofing and Enrollment
  - *Ex. exploitation:* identity fraud
  - *Ex. strengthening:* more/stronger evidence
- Authentication
  - *Ex. exploitation:* account takeovers
  - *Ex. strengthening:* multi-factor authentication (MFA)
- Federation and Assertions
  - *Ex. exploitation:* assertion modification or redirect
  - *Ex. strengthening:* trust agreement, injection protection

Considerations: Security, Equity, Privacy, Usability



Sources: NIST 800-63 series, FATF Digital Identity Guidance, March 2020

Identity in Finance – "Knowing Your Customer" (KYC)

Generally a term referring to a variety of measures (some rules-based, some risk-based) to inhibit money laundering and fraud as well as to understand the risk profile of one's customer

Example elements:

- Establish identity, form a reasonable belief that it is real and belongs to customer
- Due diligence for high-risk customers
- Transaction and risk monitoring

DEFI IDENTITY LANDSCAPE

Compliance + KYC/AML

Fireblocks

sealance

UBI

WORLDCOIN

PROOF OF HUMANITY

Standards

Verite

W3C

NIST

Sybil Resistance

SIGN IN WITH ETHEREUM

ETHEREUM NAME SERVICE

PROOF OF HUMANITY

brightID

WORLDCOIN

Reputation

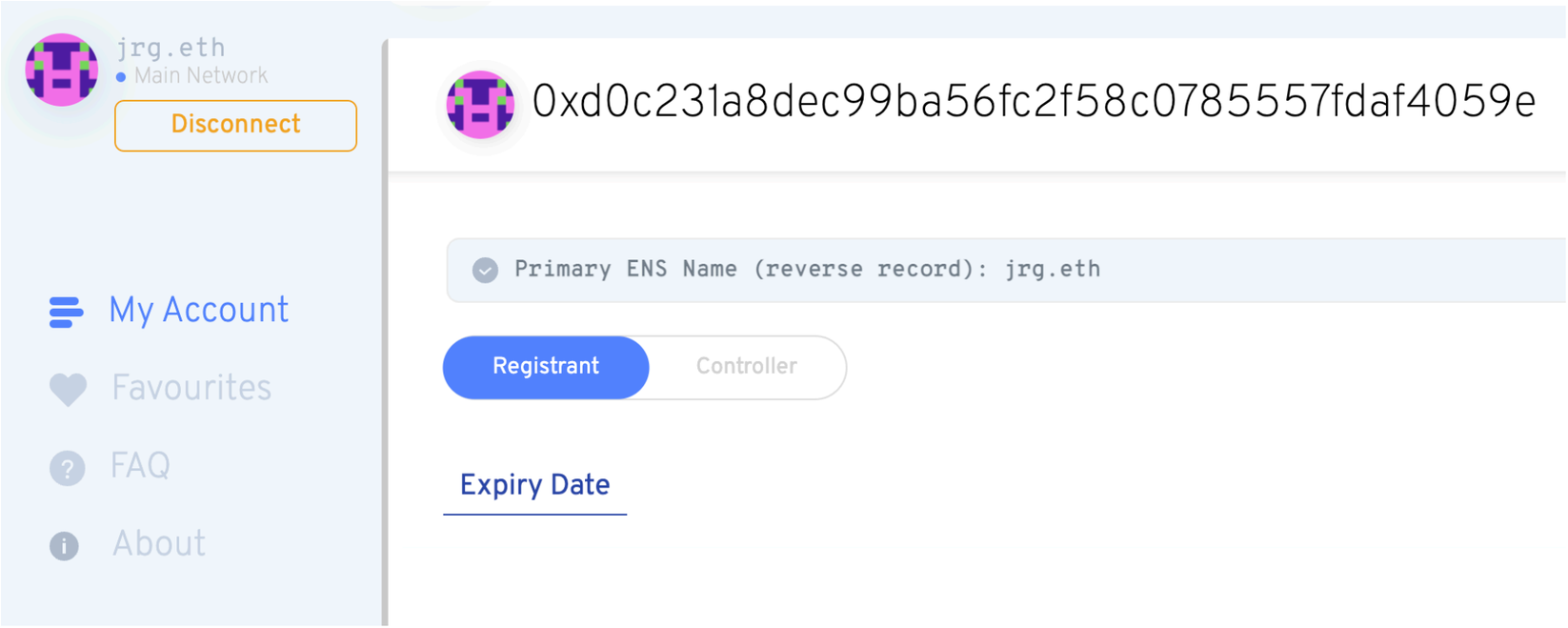
POAP

ETHEREUM NAME SERVICE

brightID

RabbitHole

EXAMPLE IDENTITY PRODUCT - ENS



- With Ethereum Name Service, users can self-identify and publicly affiliate with an Ethereum wallet address
- This allows users to prove their on-chain activity, including participating in open source governance processes; usage of products and protocols; ownership of art and collectibles; and more

PRIVACY LANDSCAPE

Private Payments –compliance emphasis

Zcash

ESPRESSO SYSTEMS

IRON FISH

PRIVACY POOLS

Private Payments – full privacy emphasis

MONERO

tornado CASH

Private Smart Contracts

Aleo

Aztec

Configurable Privacy

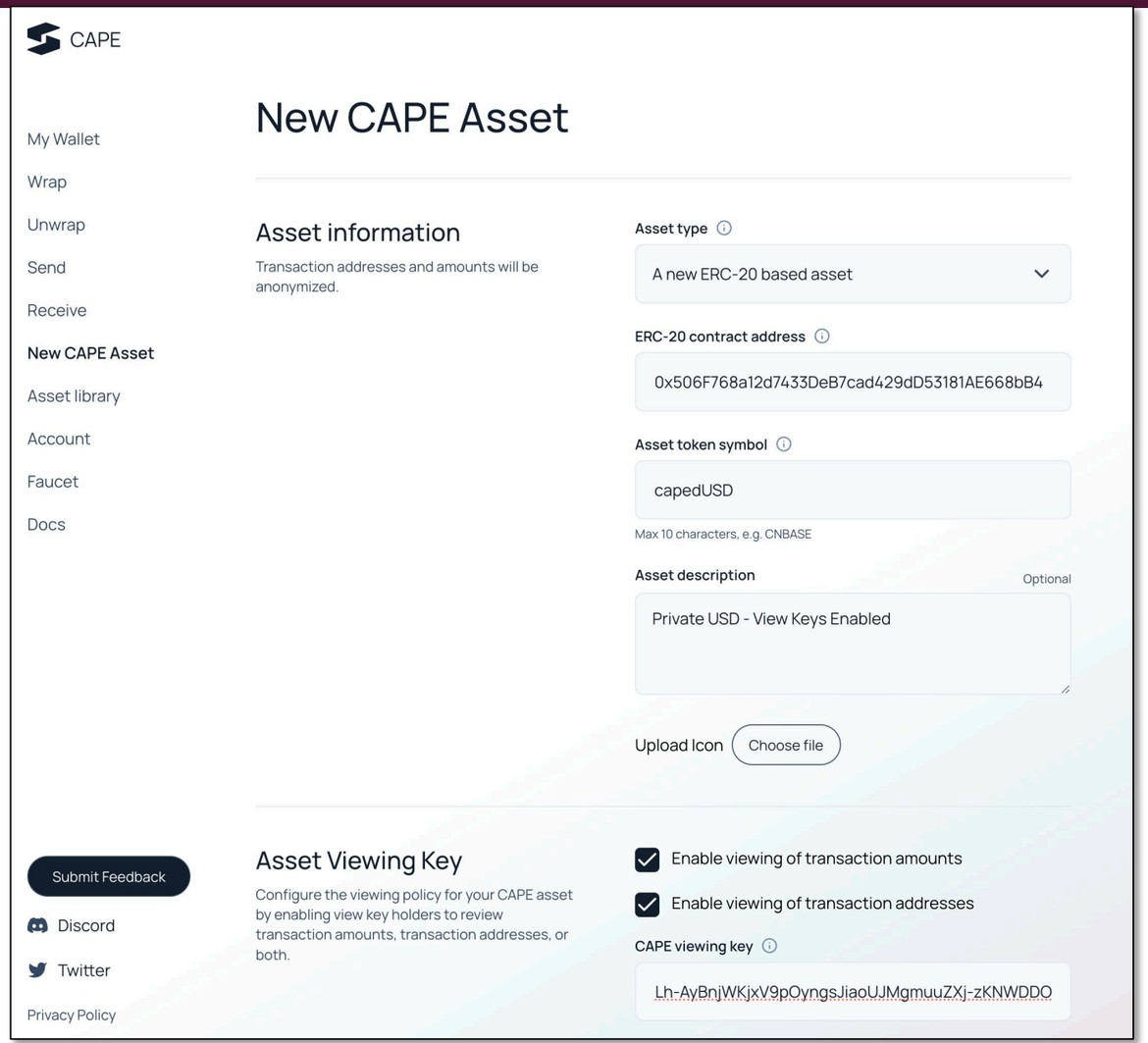
ESPRESSO SYSTEMS

Private DeFi

ESPRESSO SYSTEMS

Aztec

EXAMPLE PRIVACY PRODUCT - CAPE



- With CAPE, asset creators can create versions of their assets that have customized privacy guarantees, to meet their risk requirements
- For example, a stablecoin provider can offer users a version of their stablecoin which is private to the general public, but the stablecoin organization can retain insight into the full transaction graph (addresses, amounts, etc.)

SELF-CUSTODY LANDSCAPE (UNHOSTED WALLETS)

Hardware Wallets

Ledger

TREZOR

Browser-Based Wallets

METAMASK

coinbase | Wallet

WalletConnect

Multi-Party Computation Wallets

SEPIOR

ZenGo

Fireblocks

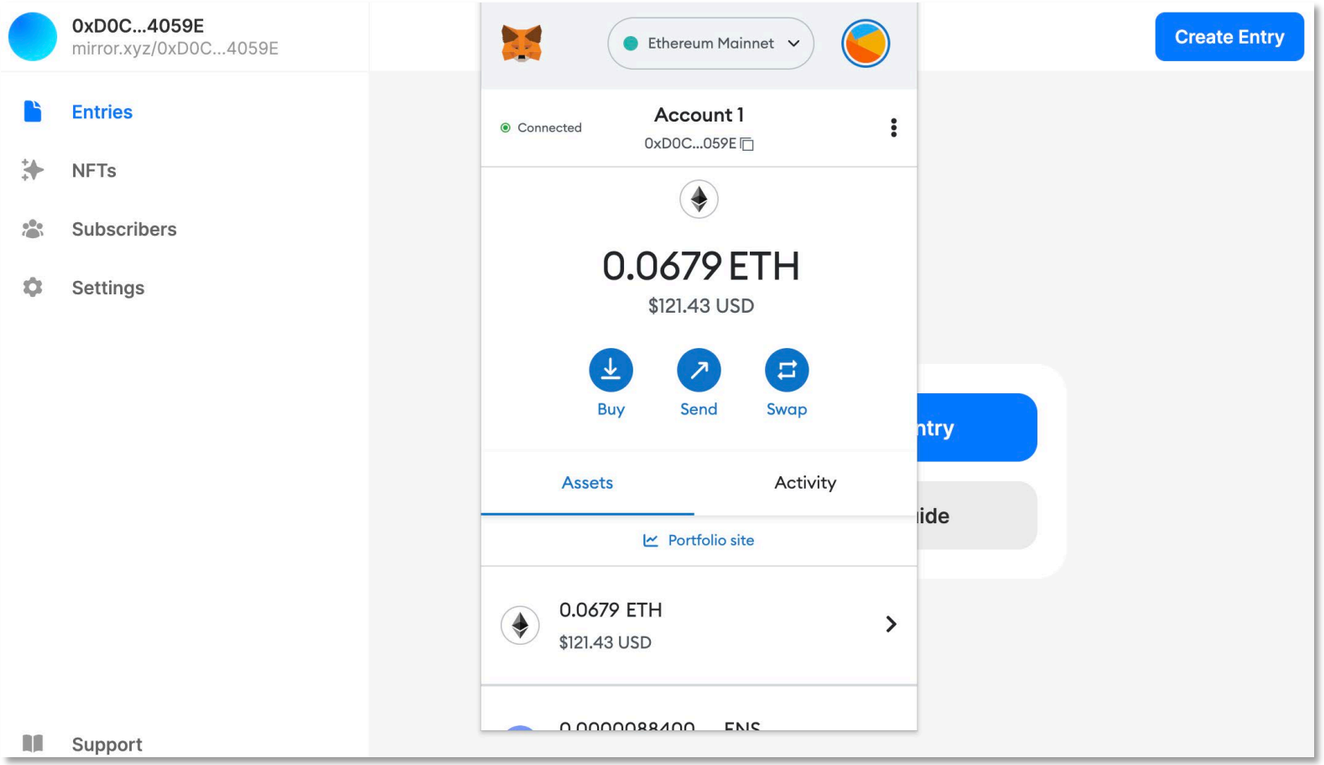
Mobile Wallets

rainbow

Blockchain.com

coinbase | Wallet

EXAMPLE WALLET PRODUCT - METAMASK



- Metamask offers a gateway to decentralized applications, right in the browser
- Metamask pops up as a plug in, acting as a universal log-in to be able to use and access decentralized finance, social, and media applications
- Shown here with decentralized blog / media application Mirror.xyz

IDENTITY, PRIVACY, AND UNHOSTED WALLETS – ISSUES AND IN THE NEWS

Bill Hughes : wchughes.eth 🦊
@BillHughesDC

🚨🚨🚨Next Wednesday, a group of EU parliament members will decide whether to support a BAN on peer-to-peer crypto transfers in the course of business above a certain dollar figure. Their support would pave the way to this becoming law that EU countries must enforce.

7:24 PM · Mar 17, 2023 · **36.7K** Views

Concerns raised over Worldcoin to 'data collection'

Sean Dickens
October 22, 2021 · 3 min read

Concerns have been raised in the crypto community over the upcoming launch of Worldcoin and its alternative approaches to data collection and 'fair distribution' of the asset.

CoinDesk

Policy

UK Government Backtracks on Unhosted Wallet Data Collection Proposal

The government said it didn't make sense to require all senders of funds to private crypto wallets to collect recipients' identification details.

By Nikhilesh De · Jun 20, 2022 at 5:22 p.m. · Updated Jun 20, 2022 at 5:31 p.m.

PRESS RELEASES

U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash

CoinDesk

Policy

Unhosted Crypto Wallet Rules Will Allow Innovation, US Treasury Official Vows

Storing crypto anonymously outside regulated venues lets people bypass sanctions and anti-money laundering checks, Deputy Secretary Wally Adeyemo said at Consensus 2022.

By Jack Schickler · Jun 10, 2022 at 6:51 p.m. · Updated Jun 10, 2022 at 8:41 p.m.

DRIVING TOWARDS STANDARDS & CLARITY

- Identity:
  - ***Define key features –*** What features of a digital identity system do we want to see (and not want to see): portability, privacy, verifiability, equity and equality of access, recoverability, etc?
  - ***Establish use cases –*** What use cases do we care about (KYC/AML, "Sybil resistance", proof-of-humanity, etc)?
  - ***Traditional identity fixes needed for defi –*** What issues exist in traditional identity systems that have to be fixed to prevent decentralization of the same identity problems in “tradfi” (e.g., identity verification, prevalence of verifiable credentials, KYC/reliance, etc.)?
  - ***Ensure responsibility in the ecosystem –*** What does responsibility and accountability for a decentralized identity system look like?

DRIVING TOWARDS STANDARDS & CLARITY

- Privacy:
  - ***Incentivizing development for data protection and appropriate discoverability –*** How to encourage or enable builders to protect user privacy, without sacrificing the ability of government and industry to detect, prevent, and disrupt criminal use and national security threats?
  - ***Prioritizing and promoting tech with protections –*** How to engage, protect, and encourage builders and innovators without condoning products that abet threatening actors?

- Unhosted wallets:
  - ***Calibrating role, treatment, freedom, and responsibility of builders –*** How to avoid creating undue burden on builders of open source wallet software?
  - ***Examining how risk, accountability, and discoverability should work in evolving systems –*** What kind of identity system enables proper discoverability of certain information (to which counterparties/authorities?) related to unhosted wallets in a system……..
    a) that largely relies on central parties and cashout points?
    b) that relies largely on decentralized networks and less need for cashout points?
    c) where the unhosted wallet holds financial assets and non-financial assets?

QUESTIONS?

Understanding Crypto Markets Security

Dan Guido - CEO, Trail of Bits

Trail of Bits

- We help solve the hardest challenges in software security
- Unmatched expertise: 140 research engineers w/ 20 in blockchain security
- Worked with DARPA, DoD, tech, and entire blockchain industry
- Have secured internal operations and blockchain code
- CEO: Product of a CISA/SFS grant, dedicated to getting software right

Things are not what they seem

Perception

- Everyone is getting hacked and losing millions
- The industry is awash in scams and schemes
- Security is mostly an afterthought

Reality

- Very difficult for orgs to keep up
- Industry is dominated by awful marketing
- Some of our clients are the most mature and security-conscious companies we work with

The field moves fast

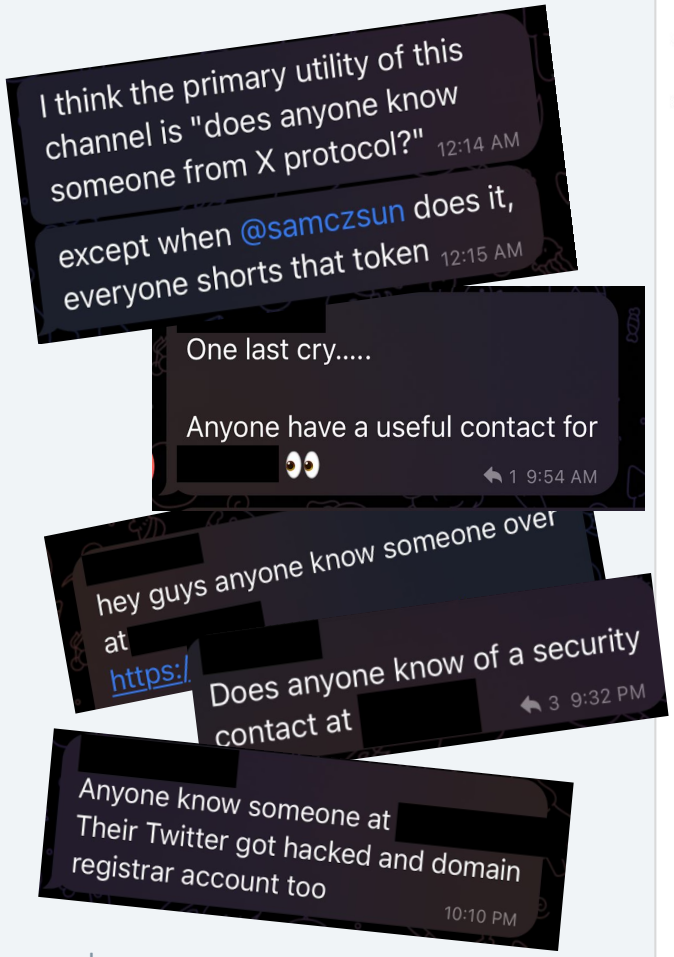
- A firm six months behind the curve on security is already woefully behind, we ourselves can barely keep up
- Standards in other industries - NIST CSF, SOC-2, PCI - don't and won't work here
- Today looks nothing like ICOs of 2017: bridges, L2s, DeFi, composability
- Criminals have also become more resourceful and sophisticated: composability bugs, flash loans, price oracle manipulation

The problems we're solving today didn't exist 5 years ago

Before ~2020	After ~2020
• Arithmetic overflow • Lack of access controls • Reentrancy	• Price Oracle Manipulation • Slippage • Cross contract reentrancy • Third party integrations

Information is public and platforms are shared

- Breaches on public on social media before orgs can react; Twitter, Discord, Telegram will know instantly
- Opportunity to learn – you can walk-through blockchain attacks step-by-step
- Inverted view on what is ‘secret’ - all contracts and transactions are inspectable by anyone, by design

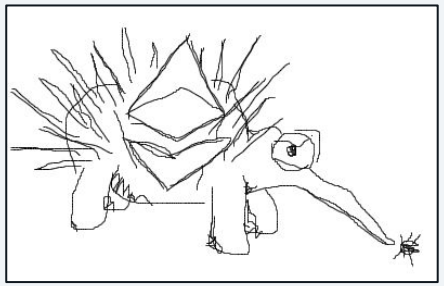


rekt

1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477,000,000 | 11/12/22
5. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
6. **Euler Finance - REKT** *Sherlock*
   $197,000,000 | 03/13/2023
7. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
8. **Nomad Bridge - REKT** *N/A*
   $190,000,000 | 08/01/2022
9. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
10. **Wintermute - REKT 2** *N/A*
    $162,300,000 | 09/20/2022

The bar is higher for blockchain

- We're building blockchain with stone tools
- Every code change is critical – safe today doesn't mean safe tomorrow.
- Blockchain code requires rocket-level safety assurances
- AI isn't going to save blockchain security; need a scalpel, not a paintbrush
- Existing best practices are necessary but insufficient: we need more research



SLITHER

MANTICORE

Summary

Key Takeaways

- Blockchain companies are motivated to fix security issues and many are very security-conscious.
- Blockchain's security foundation shifts incredibly fast and requires holistic understanding of financial and technological concepts
- Public nature of blockchain presents enormous learning opportunity
- Improved tooling and continuous testing is deeply needed; motivation and desire is not enough

… So how do we have a conversation about improving controls?

Does your protocol pass The Rekt Test?

Our checklist allows protocols to examine their own procedures and create best practices.

- ❑ Have you documented all actors, their roles, and their privileges?
- ❑ Does your key management system require multiple humans and physical steps?
- ❑ Do you have a written and tested incident response plan?
- ❑ Have all employees undergone positive identification and background checks?
- ❑ Does someone on your team have security defined in their role?
- ❑ Does access to production systems require hardware security keys?
- ❑ Do you use the best automated tools for discovering security issues in your code?
- ❑ Have you defined key invariants for your system and do you test them on every commit?
- ❑ Have you received an external audit and do you run a vulnerability disclosure or bug bounty program?
- ❑ Have you documented all the external services, contracts, and oracles you rely on?
- ❑ Have you documented the best ways to attack your own system?
- ❑ Have you considered and mitigated avenues for abusing users of your system?

Resources

The Rekt Test

Are blockchains decentralized?

246 findings from audits

65 open source tools

Smart contract best practices

Contact

@dguido

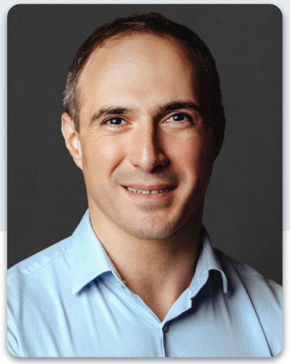
dan@trailofbits.com

trailofbits.com

Fireblocks

Brief Overview of Real World Crypto Hacks

For CFTC TAC 3/2023



Michael Shaulov
CEO & CO-FOUNDER

Head of Mobile & Cloud, Check Point
grew to 2000+ customers

CEO & Co-founder, LACOON
acquired by Check Point

Fireblocks

A platform that enables financial institutions to work with digital assets in secure and simple way

Fireblocks Solutions for Financial Institutions

- Treasury Management
- Institutional Custody
- Digital Asset Trading
- Tokenization of Real World Assets

TRUSTED BY INDUSTRY LEADERS

1,800+
customers

$4T+
transactions secured

90M+
wallets

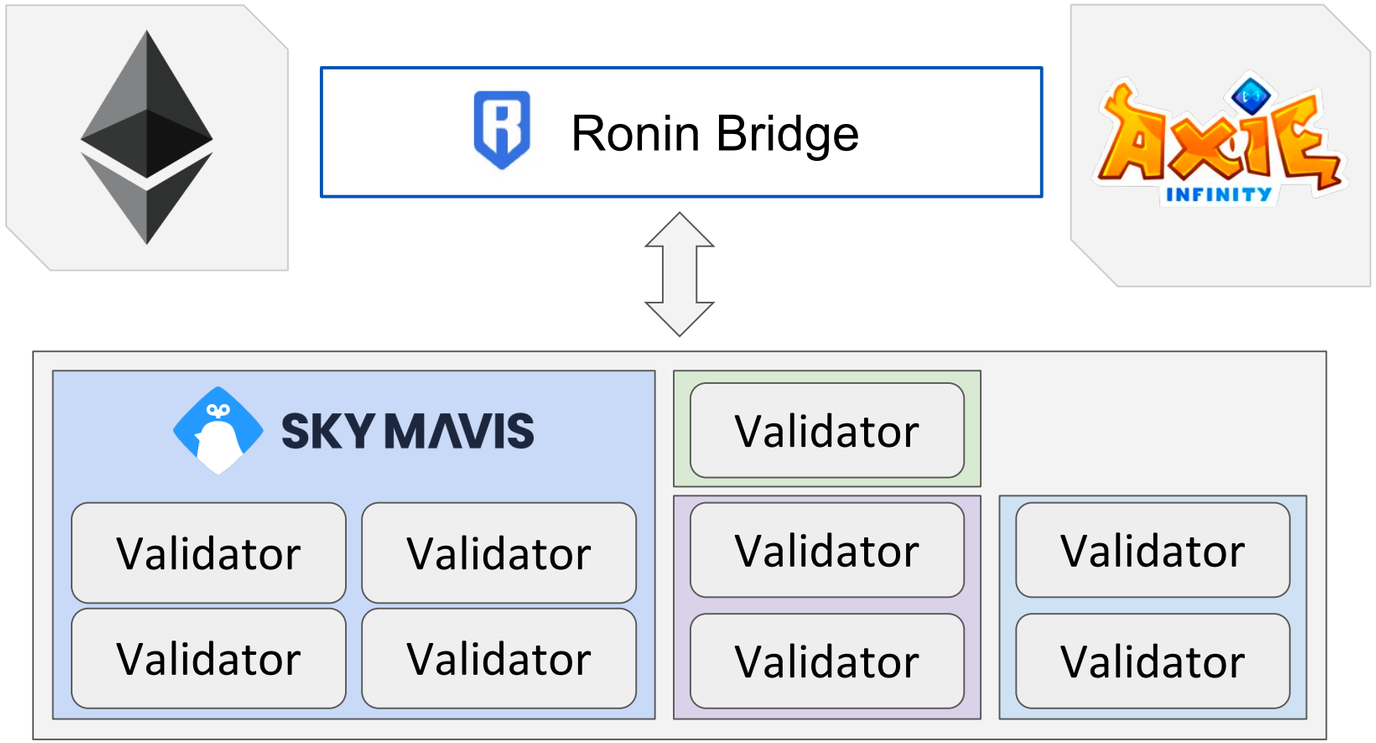
Agenda

We will review the following hacks:

1. Key management: Ronin
2. Man-in-the-Middle: Badger
3. Smart Contract: Euler

The Ronin Bridge

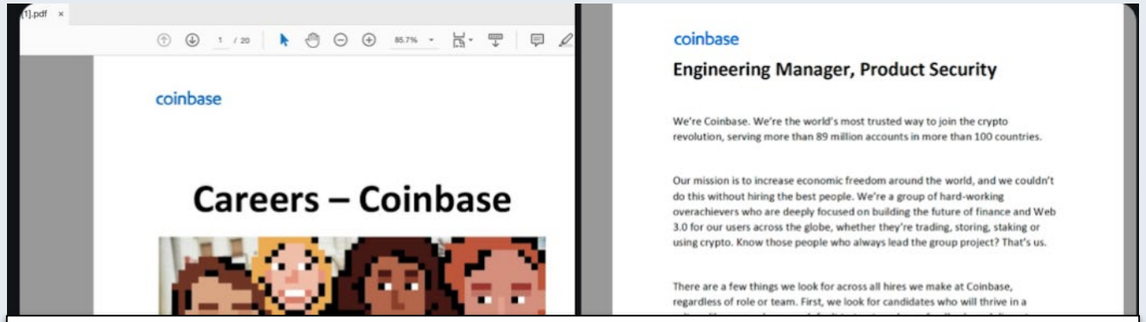
- Sky Mavis created Axie Infinity - an NFT Play-to-Earn game
- Used their own high-performance chain for gaming UX
- Ronin Bridge connecting the side-chain to Ethereum
- Controlled by a 5/9 multisig; Sky Mavis had 4 private keys



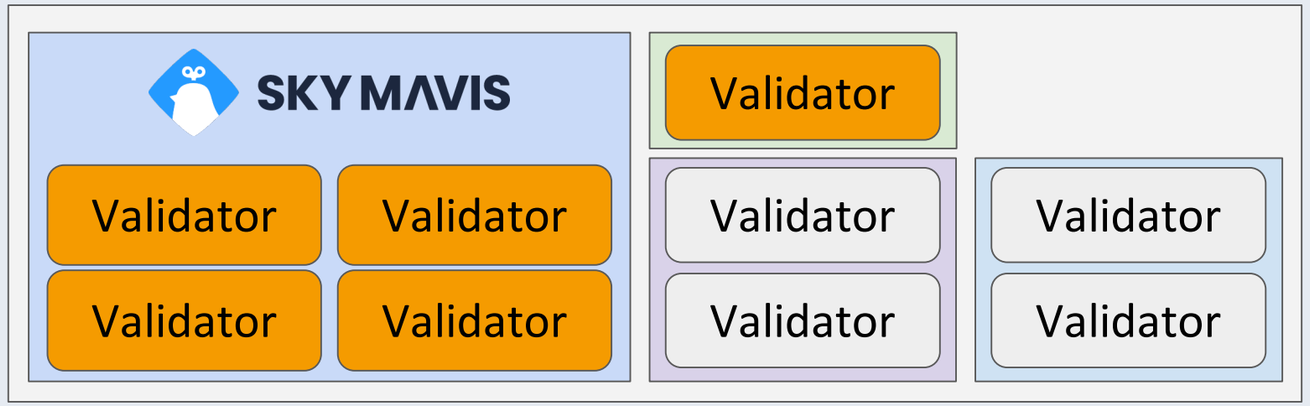
The Ronin Breach

- March 23rd 2022
- Targeting Sky Mavis engineers
- LinkedIn reachout & interviews
- Dream Job offering .pdf.exe
- Lateral movement to keys
- Axie DAO collab - auto signing

- Transfer funds $650mm
  - 173K ETH
  - 25.5M USDC
- Attack identified 5 days later

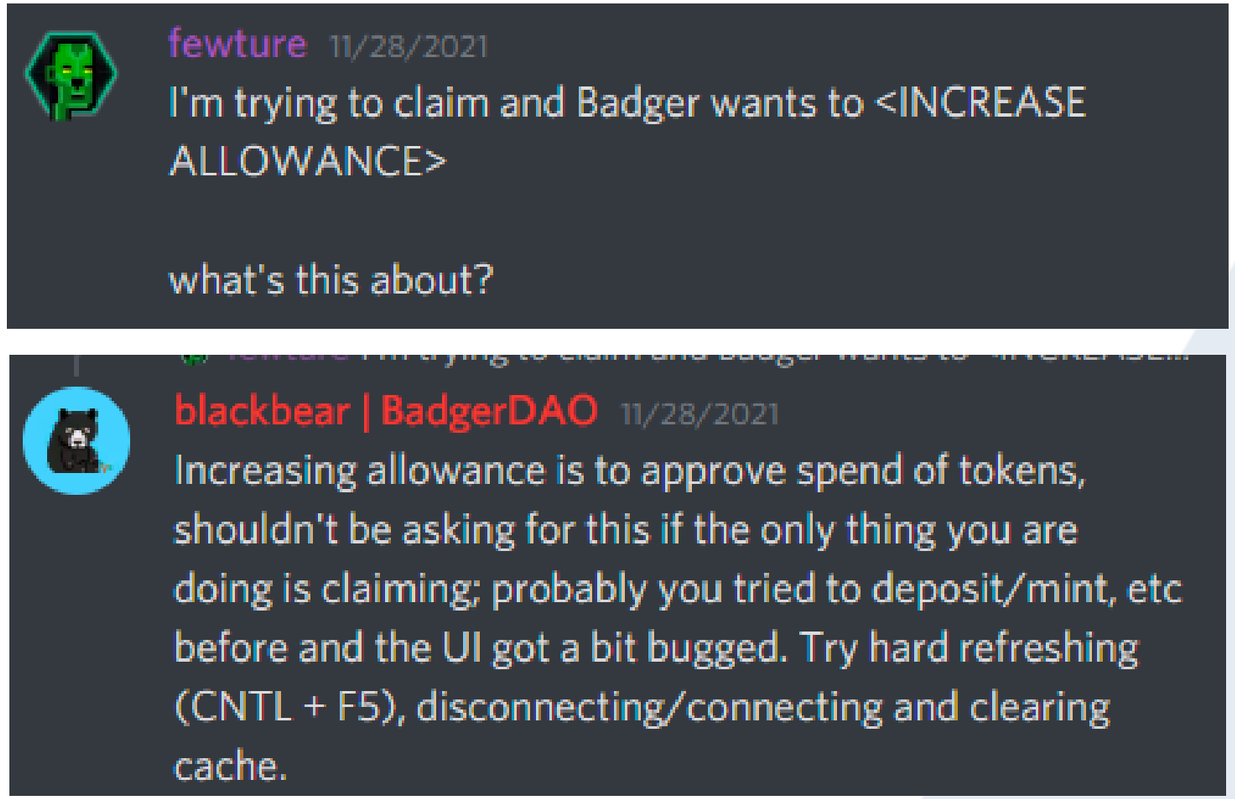


How a fake job offer took down the world's most popular crypto game



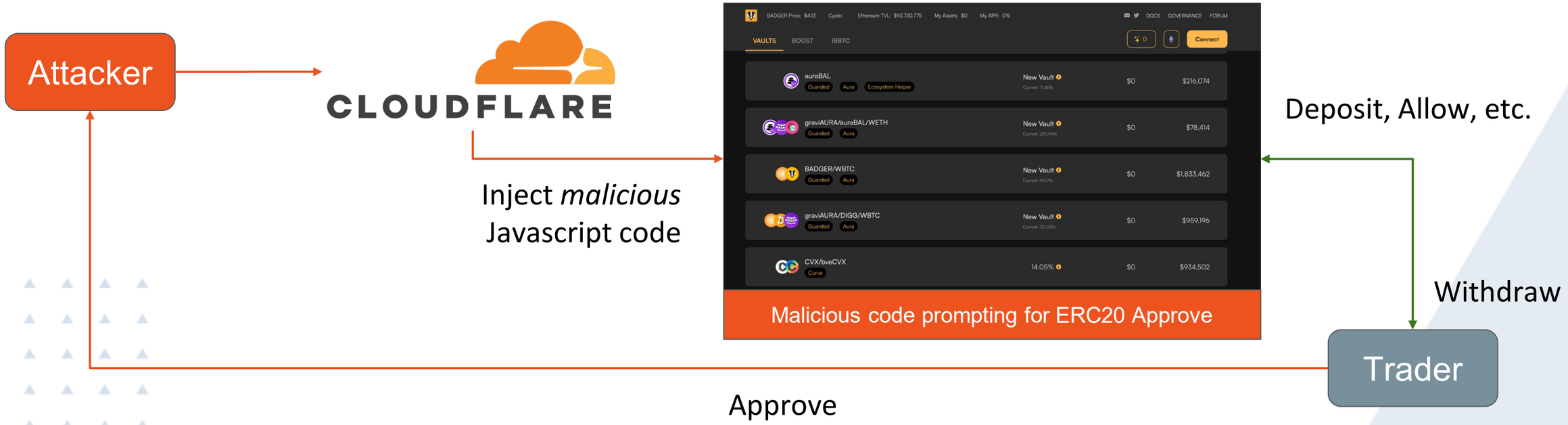
BadgerDAO - Background

- Badger dApp - usage
- Using Cloudflare for managing dApp’s front-end



BadgerDAO - Hacked

- Vulnerability with Cloudflare, allowing to get access to API keys
- Attacker gained access to Badger's front-end, injecting a malicious script
- Approve farming starting Nov. 20th for two weeks
  - Would ask users to approve attacker's control of their tokens
- Trying to stay hidden - filtering out addresses belonging to Badger's admins
- December 2nd, 2021 - attacker cashed out all approvals



Euler Finance - The Protocol

- Trading/lending protocol
- Users can enter a debt, trade x10 of their collateral
- *eToken - collateral token, dToken - debt token.

Euler Finance - What Went Wrong?

- Tuesday March 14th 2023
- donateToReserves lacked liquidity checks
  - Attacker created negative eTokens:dTokens ratio in their first contract
- By deploying a flash-loan and depositing tokens in Euler platform, loaning other tokens and donating some of the eTokens* to the reserves using donateToReserves, the attacker was able to use their second contract to liquidate the first -> making profit

Thank you

FOR MORE INFORMATION

FIREBLOCKS.COM

CFTC

COMMODITY FUTURES TRADING COMMISSION

Topic 2: Ensuring Cyber Resilience in Financial Markets

Treasury/OCCIP Efforts To Support Sector Resilience

OCCIP

Office Of Cybersecurity & Critical Infrastructure Protection

TLP:GREEN

CFTC
Technology Advisory Committee
March 22, 2023

Presentation Overview

Topics
OCCIP Introduction
Treasury Cloud Report
Cyber Incident Communications Playbook
ION Markets Incident

TLP:GREEN

OCCIP Purpose & Goals

Purpose

- Improve the security and resilience of the financial services sector by serving as the central node for information related to all hazards threats, building resilience through exercises, and responding to incidents when they do occur.

Goal

- Ensure the U.S. maintains the world's most secure and resilient financial system by spearheading whole-of-government efforts to increase the cybersecurity and resilience of the American financial system.

Cloud Report Background

Coordination with FBIIC

- Last year, Treasury started working on a report on cloud services and potential implications for operational resilience, in coordination with members of the Financial and Banking Information Infrastructure Committee, or FBIIC.

Stakeholder and Expert Consultation

- The report was developed with the assistance of subject matter experts at the U.S. financial regulators. It also reflects input from experts at the Cybersecurity and Infrastructure Security Agency, National Institute of Standards and Technology, the Office of the National Cyber Director, and the National Security Council, as well as nearly 50 interviews with private sector stakeholders, trade associations, and think-tanks.

Primary Findings on Cloud Adoption

Range of Maturity in Terms of Cloud Adoption

- Cloud services is no longer an emerging technology and is widely used for email and video conferencing, and now financial institutions are starting to use it for core operations.

Cloud Adoption Expected to Persist

- Some firms, particularly some smaller firms, do not see cloud adoption as a choice, since other third-party vendors are discontinuing their on-premises solutions in favor of cloud-based solutions.

Benefits of Adoption

Potential Benefits

When configured correctly, Cloud Services can provide significant benefits in terms of redundancy, scalability, and security.

1. **Redundancy:** Cloud services offer physical redundancy with the potential to operate from multiple “availability zones,” which are physically or logically isolated data centers that host cloud services.

2. **Scalability:** Cloud services can be procured and deployed much more rapidly than traditional private networks.

3. **Security:** The security capabilities for public cloud services could generally match or exceed their on-premises capabilities.

Challenges with Adoption

Treasury noted six main challenges to greater cloud adoption by FIs:

1. **Transparency.** Financial Institutions lack some information necessary to conduct due diligence and monitoring of CSPs, and CSPs note obstacles to providing such information at scale.

2. **Gaps in Expertise and Tools.** The *shared responsibility model* calls upon FIs to have necessary expertise, tools, and information.

3. **Exposure to Potential Operational Incidents, Including from Incidents Originating at a CSP:** Cloud services are still vulnerable to operational incidents like any technology utilized by financial institutions.

4. **Potential Impact of Market Concentration on the Sector's Resilience:** Because cloud adoption is concentrated, a large system failure or data breach at one of these CSPs could impact the sector.

5. **Dynamics in Contract Negotiations:** Treasury discovered asymmetry in bargaining power in favor of CSPs, especially among small institutions.

6. **International Landscape and Regulatory Fragmentation.** FIs report that consistent adoption of cloud across jurisdictions is hindered by data localization requirements and inconsistent regulatory frameworks. Foreign regulators will start to oversee CSPs, which could result in negative impacts to all customers.

Next Steps – Strategic Vision

The next steps taken by Treasury will be guided by its <u>Strategic Vision for Supporting the Resilience of the Financial Sector's Use of Cloud Services</u>.

This articulation of Treasury's long-term objectives includes:

- A **Preamble** that focuses on common interests shared by all stakeholders and announces principles for collaborating with such stakeholders on addressing issues that could impact the operational resilience of the sector.
- Principles in terms of **risk assessment and mitigation.**
- Priorities in terms of **sector-wide concentration.**
- Objectives in terms of domestic and international **collaboration and coordination**.

Next Steps – Cloud Services Steering Group

Treasury will set up an interagency Cloud Services Steering Group to coordinate on issues raised in this report. Reporting to both FSOC and FBIIC.

We anticipate this will be a multi-year effort. Key objectives include:

- Develop common definitions and terms;
- Enhancement of interagency information sharing and risk management pertaining to enhancement of both the financial services sector and cloud service providers;
- Incident response involving cloud services, such as updating processes to expand communication channels between U.S. financial regulators, CSPs, and financial institutions; and
- Sector-wide measurement of the concentration of critical uses of cloud services and similar third-party services.

Next Steps – Stakeholder Engagement

Treasury will pursue continued engagement with the private sector on various issues raised in the report, including issues related to risk management practices and contracting.

- Treasury will lead ongoing engagement with the Financial Services Sector Coordinating Council (FSSCC), which will set up a working group to tackle cloud issues from the industry perspective.
- Initial deliverables will be Cloud Adoption Framework (Cyber Risk Institute) and Cloud Contracts Best Practices (SIFMA).
- Treasury will promote cooperation between CSPs and the financial sector, including through the development of best practices and a framework for cloud adoption.

A key objective in the near and medium term is for the public sector and the financial sector to provide more actionable feedback for individual CSPs.

Background and Context

- Following the stand-up of the Unified Coordination Group (UCG) by DHS on February 22, 2022, US Treasury engaged with financial sector organizations to develop a joint playbook for how the USG and industry may communicate and engage during incident response and recovery in the current period of heightened geopolitical tensions.

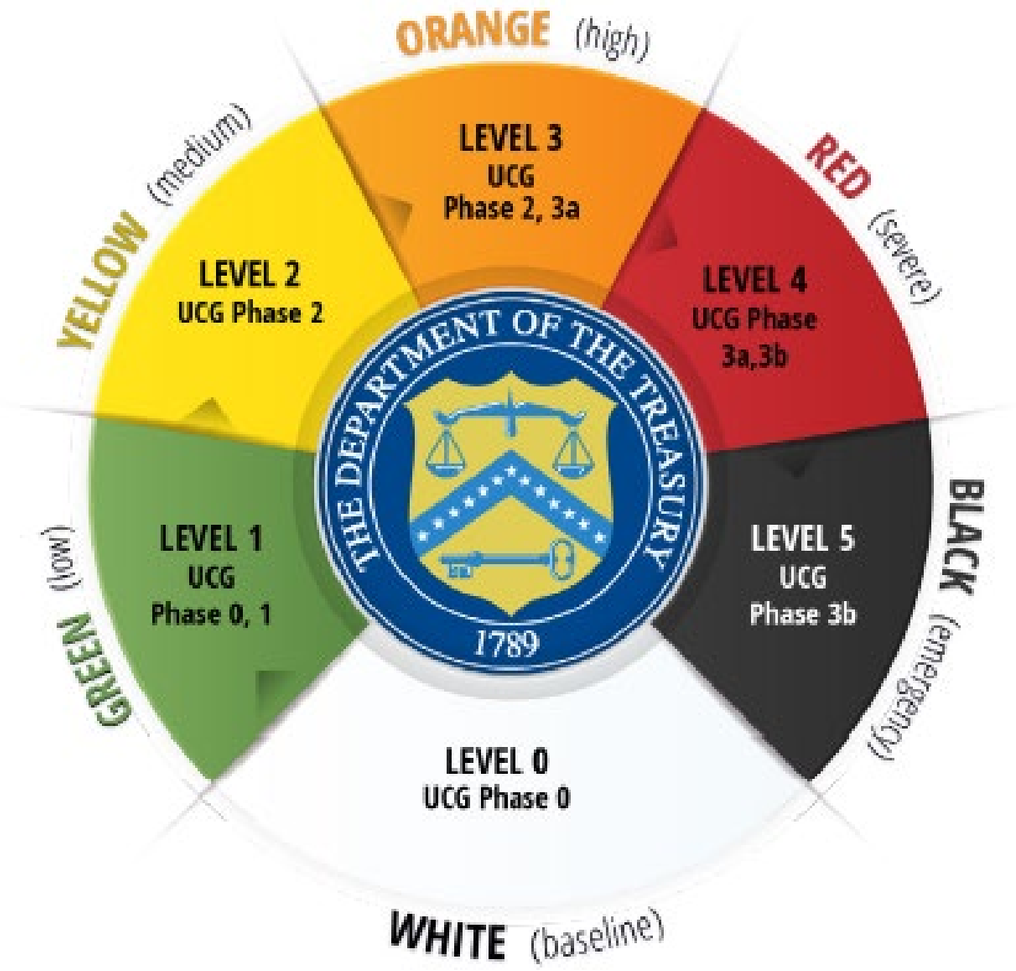
- Developed for use in response to the heightened vigilance and activity generated by the Russia-Ukraine conflict, this description will be primarily utilized to coordinate communication related to specific incidents/events observed in the financial services sector and other critical sectors that have systemic impact on financial services.

- The playbook leverages the Cyber Incident Severity Schema developed by the U.S. Government and aligns potential USG actions and industry needs with each of the five levels within the schema. For incidents at each level of the schema, the description includes an outline of expected government coordination and communications actions, examples of anticipated business impacts for such an incident, and a representative list of extraordinary requests that the financial services sector may issue to USG partners.

Escalatory Phase Charts

- The UCG created an escalatory phase chart (phase 0 to 3b) contemplating specific escalatory phases specific to the Russia cyber threat

- The UCG phases were overlayed onto the FBIIC Cyber Incident Severity level schema to provide extra context for firms' cyber threat level analysis for each UCG threat phase.



TLP:GREEN

Summary - Industry Asks of Government in Response to Various Cyber Scenarios

- Maintain clear, direct channels of communication between USG and firms
- Coordinate public messaging at market speed, especially to maintain public confidence in the financial system and to minimize false presumption of market instability
- Protect critical cyber ops resources from disruption by coordinating and minimizing the duplication of regulatory and government inquiry; firms will engage regulators as part of their response planning
- Coordination, working with existing market solutions, of changes to normal market hours or operation _ emergency planning for banking services/markets/trading/settlement disruption
- Share intelligence and early warning wherever possible (including exchange directly among analysts to provide context)
- Prioritize Section 9 firms in the restoration/reconnection plans for critical infrastructure (FedWire, CHIPS, DTC, etc.) and cross sector dependencies (ISP, Telecom, Electricity)
- Extend hours for critical infrastructure processing – i.e., FedWire, CHIPS, DTC, etc.
- Provide temporary regulatory relief/forbearance – capital/liquidity/reporting/cyber regulation/resolution triggering
- Authorize firms to bypass pre-payment sanctions screening to avoid systemic disruptions in payments markets
- Implement flexible emergency lending capacity and other solutions for injecting liquidity into financial system
- Notify firms of SIFMU disruption or impact

ION Markets Incident: Beginning

Overnight January 30-31, 2023

- ION Markets division of ION Group struck by Lockbit ransomware
- Lockbit ransomware disabled *hosted* services used to clear trades among derivatives, fixed income, and foreign exchange traders.
    - At outset it was believed that all of ION Markets' services had been disrupted

January 31, 2023

- Disruption of ION's trade-clearing services results in growing backlog of trades
- Futures Industry Association (FIA) begins coordination calls among members
- By end of day, there are also delays in reports from exchanges to their regulatory agencies.

Concerns

Sector Risks

- Possible liquidity crunch, if a sufficient number and size of firms are forced to default

Sub-Sector Risks

- Increased market fragility for next several weeks or months
- Degradation of trading speed
- Failure to comply with regulatory reporting obligations

ION Markets Incident: Assessing Impact from OCCIP's Perspective

Unknowns, as of the morning of February 1

- UNK number and type of ION's services disrupted
- UNK number and size of impacted Financial Institutions
- UNK size of outstanding debt held by impacted traders and size of creditors

Knowns, as of the morning of February 1

- Disruption caused "National-level" impact among dispersed group of traders
- "Significant" impact to *sector* business critical services
- Active, financially-motivated cyberattack

Assessment

- Based on known information and likely estimates, OCCIP assessed the ION Incident as a Level 2, Medium severity incident (morning of February 1, 2023).

OCCIP and USG Response

February 1, 2023

OCCIP participates in series of calls with private and public sector stakeholders

Findings

- Calls reveal that 42 firms have been impacted
  - Firms are of the small-to-medium category
- Open communication among traders, exchanges, and regulators
- Strong compensatory measures have been enacted by traders
- Mutual aid among traders, exchanges, and lenders
- Regulatory scrutiny and flexibility is present
- Treasury issues press statements to calm public/markets

Conclusion

- Based on these findings, OCCIP determined that there is no longer a “systemic risk” posed by this incident.
- Severity downgraded to Level 1, Low (close of business, February 1, 2023).

U.S. Treasury OCCIP Contacts

Todd Conklin
Deputy Assistant Secretary
Cybersecurity and Critical Infrastructure Protection
Todd.Conklin@treasury.gov

Tim McCabe
Deputy Director
Sector Resilience
Timothy.McCabe@treasury.gov

Incident Mailbox
Occip-coord@treasury.gov

TLP:GREEN

THANK YOU…

TLP:GREEN

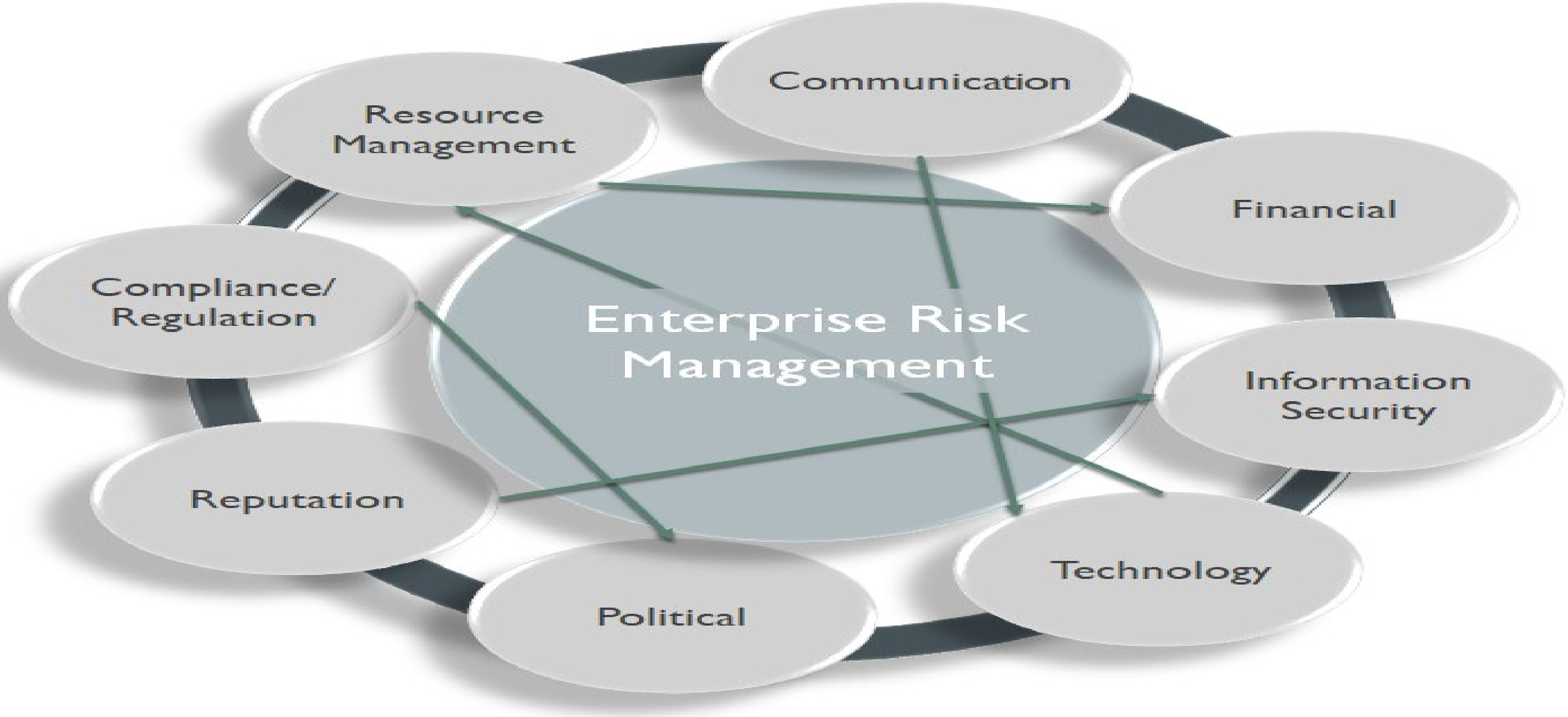
Managing Cybersecurity Risks
CFTC TAC

Kevin Stine, NIST

March 22, 2023

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Managing Risks to the Enterprise



Cybersecurity Framework

- Common and accessible language
- It's risk- and outcome-based
- It's meant to be paired
- It's a living document
- It's adaptable to many technologies, lifecycle phases, sectors and uses
- Guided by many perspectives – private sector, academia, public sector

Helping Organizations Better Understand, Communicate, Manage, and Reduce Cybersecurity Risks

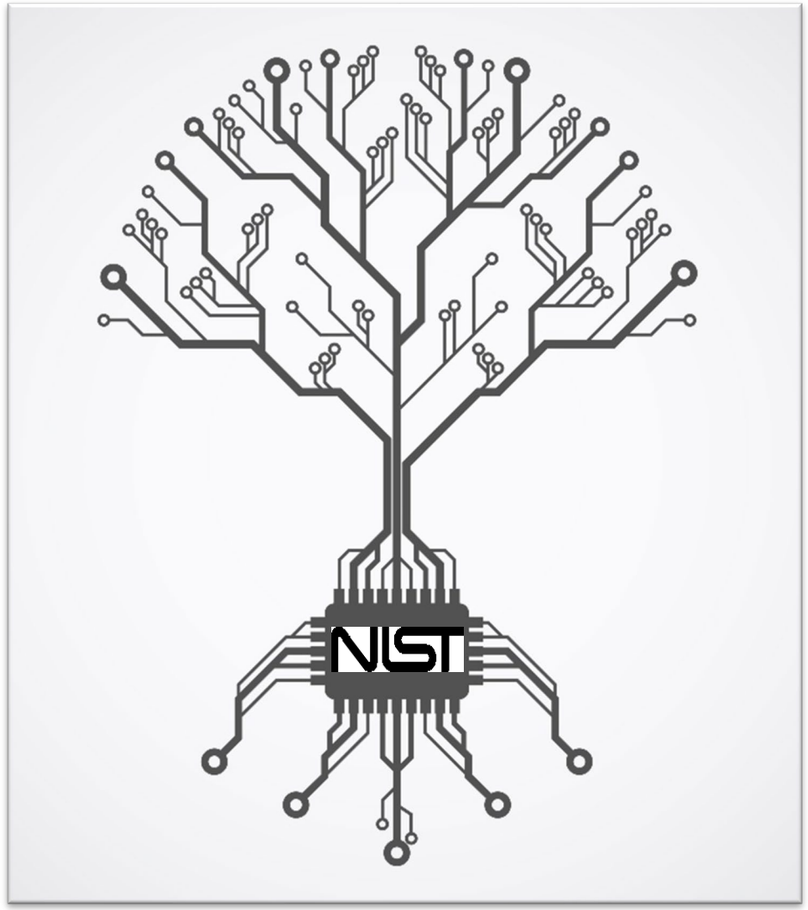
CSF 2.0: Potential Changes

Among other improvements, CSF 2.0 will:

- emphasize the importance of **cybersecurity governance**
- emphasize the importance of **cybersecurity supply chain risk management** (C-SCRM)
- advance understanding of **cybersecurity measurement and assessment**

Resources of Interest

- **Cybersecurity Framework** – https://www.nist.gov/cyberframework
  - CSF 2.0 Update Process
  - Quick Start Guide
  - Resources
- **Cybersecurity Supply Chain** – https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management
  - Cybersecurity SCRM Practices
  - Key Practices in Cyber SCRM: Observations from Industry



Thank You

NIST.gov/cybersecurity
Cybersecurity-Privacy@nist.gov
@NISTcyber

CFTC

COMMODITY FUTURES TRADING COMMISSION

Topic 3: Responsible Artificial Intelligence (AI)

THE WHITE HOUSE
WASHINGTON

Blueprint for an AI Bill of Rights

Making Automated Systems Work for the American People

Alan Mislove
Assistant Director for Data and Democracy
White House Office of Science and Technology Policy

Blueprint for an AI Bill of Rights

Safe and Effective Systems

You should be protected from unsafe or ineffective systems.

Blueprint for an AI Bill of Rights

Safe and Effective Systems

You should be protected from unsafe or ineffective systems.

Algorithmic Discrimination Protections

You should not face discrimination by algorithms and systems should be used and designed in an equitable way.

Blueprint for an AI Bill of Rights

Safe and Effective Systems

You should be protected from unsafe or ineffective systems.

Algorithmic Discrimination Protections

You should not face discrimination by algorithms and systems should be used and designed in an equitable way.

Data Privacy

You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used.

Blueprint for an AI Bill of Rights

Safe and Effective Systems

You should be protected from unsafe or ineffective systems.

Algorithmic Discrimination Protections

You should not face discrimination by algorithms and systems should be used and designed in an equitable way.

Data Privacy

You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used.

Notice and Explanation

You should know when an automated system is being used and understand how and why it contributes to outcomes that impact you.

Blueprint for an AI Bill of Rights

Safe and Effective Systems

You should be protected from unsafe or ineffective systems.

Algorithmic Discrimination Protections

You should not face discrimination by algorithms and systems should be used and designed in an equitable way.

Data Privacy

You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used.

Notice and Explanation

You should know when an automated system is being used and understand how and why it contributes to outcomes that impact you.

Human Alternatives, Consideration, and Fallback

You should be able to opt out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter.

Listening to the American People

Adobe
American Civil Liberties Union (ACLU)
The Aspen Commission on Information Disorder
The Awood Center
The Australian Human Rights Commission
Biometrics Institute
The Brookings Institute
BSA | The Software Alliance
Cantellus Group
Center for American Progress
Center for Democracy and Technology
Center on Privacy and Technology at Georgetown Law
Christiana Care
Color of Change
Coworker
Data Robot
Data Trust Alliance
Data and Society Research Institute
Deepmind
EdSAFE AI Alliance
Electronic Privacy Information Center (EPIC)
Institute of Electrical and Electronics Engineers (IEEE)
Intuit
Lawyers Committee for Civil Rights Under Law
Legal Aid Society
The Leadership Conference on Civil and Human Rights
Meta
Microsoft
The MIT AI Policy Forum
Movement Alliance Project
The National Association of Criminal Defense Lawyers
O'Neil Risk Consulting & Algorithmic Auditing
The Partnership on AI
Pinterest
The Plaintext Group
pymetrics
SAP
The Security Industry Association
Software and Information Industry Association (SIIA)
Special Competitive Studies Project
Center
Unfinished/Project Liberty
Upturn
US Chamber of Commerce
US Chamber of Commerce Technology Engagement Center A.I. Working Group
Vibrent Health
Warehouse Worker Resource Center
Waymap

58 meetings with industry and civil society

150+ emails to public email address

30+ federal departments, agencies, and components

THE WHITE HOUSE
WASHINGTON

FROM PRINCIPLES TO PRACTICE

A Technical Companion to the Blueprint for an AI Bill of Rights

Applying the Blueprint for an AI Bill of Rights

THIS FRAMEWORK DESCRIBES PROTECTIONS THAT SHOULD BE APPLIED WITH RESPECT TO ALL AUTOMATED SYSTEMS THAT HAVE THE POTENTIAL TO MEANINGFULLY IMPACT INDIVIDUALS' OR COMMUNITIES' EXERCISE OF:

RIGHTS, OPPORTUNITIES, OR ACCESS

Civil rights, civil liberties, and privacy, including freedom of speech, voting, and protections from discrimination, excessive punishment, unlawful surveillance, and violations of privacy and other freedoms in both public and private sector contexts;

Equal opportunities, including equitable access to education, housing, credit, employment, and other programs; or,

Access to critical resources or services, such as healthcare, financial services, safety, social services, non-deceptive information about goods and services, and government benefits.

A Technical Companion
to the Blueprint for an AI Bill of Rights

1 Why this principle is important:

This section provides a brief summary of the problems that the principle seeks to address and protect against, including illustrative examples.

2 What should be expected of automated systems:

- **The expectations for automated systems are meant to serve as a blueprint for the development of additional technical standards and practices that should be tailored for particular sectors and contexts.**
- This section outlines practical steps that can be implemented to realize the vision of the Blueprint for an AI Bill of Rights. The expectations laid out often mirror existing practices for technology development, including pre-deployment testing, ongoing monitoring, and governance structures for automated systems, but also go further to address unmet needs for change and offer concrete directions for how those changes can be made.

3 How these principles can move into practice:

This section provides real-life examples of how these guiding principles can become reality, through laws, policies, and practices. It describes practical technical and sociotechnical approaches to protecting rights, opportunities, and access.

Blueprint for an AI Bill of Rights

Safe and Effective Systems

You should be protected from unsafe or ineffective systems. Automated systems should be developed with consultation from diverse communities, stakeholders, and domain experts to identify concerns, risks, and potential impacts of the system. Systems should undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards. Outcomes of these protective measures should include the possibility of not deploying the system or removing a system from use. Automated systems should not be designed with an intent or reasonably foreseeable possibility of endangering your safety or the safety of your community. They should be designed to proactively protect you from harms stemming from unintended, yet foreseeable, uses or impacts of automated systems. You should be protected from inappropriate or irrelevant data use in the design, development, and deployment of automated systems, and from the compounded harm of its reuse. Independent evaluation and reporting that confirms that the system is safe and effective, including reporting of steps taken to mitigate potential harms, should be performed and the results made public whenever possible.

WHY THIS PRINCIPLE IS IMPORTANT

- A proprietary model was developed to predict the likelihood of sepsis in hospitalized patients and was implemented at hundreds of hospitals around the country. An independent study showed that the **model predictions underperformed relative to the designer's claims** while also causing 'alert fatigue' by falsely alerting likelihood of sepsis.

- A device originally developed to help people track and find lost items has been **used as a tool by stalkers to track victims' locations in violation of their privacy and safety**. The device manufacturer took steps after release to protect people from unwanted tracking by alerting people on their phones when a device is found to be moving with them over time and also by having the device make an occasional noise, but not all phones are able to receive the notification and the devices remain a safety concern due to their misuse.

- An algorithm used to deploy police was found to repeatedly send police to neighborhoods they regularly visit, even if those neighborhoods were not the ones with the highest crime rates. These **incorrect crime predictions were the result of a feedback loop** generated from the reuse of data from previous arrests and algorithm predictions.

WHAT SHOULD BE EXPECTED OF AUTOMATED SYSTEMS

Protect the public from harm in a proactive and ongoing manner

- ❑ Consultation.
- ❑ Testing.
- ❑ Risk identification and mitigation.
- ❑ Ongoing monitoring.
- ❑ Clear organizational oversight.

Avoid inappropriate, low-quality, or irrelevant data use and the compounded harm of its reuse

- ❑ Relevant and high-quality data.
- ❑ Derived data sources tracked and reviewed carefully.
- ❑ Sensitive domains data reuse limits.

Demonstrate the safety and effectiveness of the system

- ❑ Independent evaluation.
- ❑ Reporting.

HOW THESE PRINCIPLES CAN MOVE INTO PRACTICE

- **From large companies to start-ups, industry is providing innovative solutions that allow organizations to mitigate risks to the safety and efficacy of AI systems, both before deployment and through monitoring over time.** These innovative solutions include risk assessments, auditing mechanisms, assessment of organizational procedures, dashboards to allow for ongoing monitoring, documentation procedures specific to model assessments, and many other strategies that aim to mitigate risks posed by the use of AI to companies' reputation, legal responsibilities, and other product safety and effectiveness concerns.

- **The National Institute of Standards and Technology (NIST) developed a risk management framework to better manage risks posed to individuals, organizations, and society by AI.** The NIST AI Risk Management Framework, as mandated by Congress, is intended for voluntary use to help incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. The NIST framework was developed through a consensus driven, open, transparent, and collaborative process that included workshops and other opportunities to provide input.

Extra Protections for Data Related to Sensitive Domains

- **Some domains, including health, employment, education, criminal justice, and personal finance, have long been singled out as sensitive domains deserving of enhanced data protections.** This is due to the intimate nature of these domains as well as the inability of individuals to opt out of these domains in any meaningful way, and the historical discrimination that has often accompanied data knowledge. Domains understood by the public to be sensitive also change over time, including because of technological developments. Tracking and monitoring technologies, personal tracking devices, and our extensive data footprints are used and misused more than ever before; as such, the protections afforded by current legal guidelines may be inadequate. The American public deserves assurances that data related to such sensitive domains is protected and used appropriately and only in narrowly defined contexts with clear benefits to the individual and/or society.

- **To this end, automated systems that collect, use, share, or store data related to these sensitive domains should meet additional expectations.** Data and metadata are sensitive if they pertain to an individual in a sensitive domain (defined below); are generated by technologies used in a sensitive domain; can be used to infer data from a sensitive domain or sensitive data about an individual; or have the reasonable potential to be used in ways that are likely to expose individuals to meaningful harm, such as a loss of privacy or financial harm due to identity theft.

THE WHITE HOUSE
WASHINGTON

www.whitehouse.gov/ostp/ai-bill-of-rights

The Responsible Development, Deployment, and Use of Artificial Intelligence

Francesca Rossi

IBM AI Ethics Global Leader

A brief history of AI

SYMBOLIC ARTIFICIAL INTELLIGENCE

Intelligent algorithms defined and coded by people into machines

1956

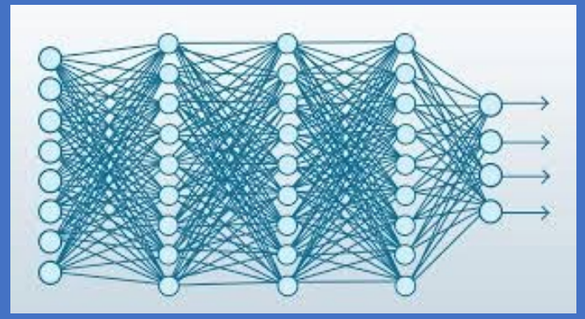
MACHINE LEARNING

Ability to learn from data, without being explicitly programmed

1980s

DEEP LEARNING

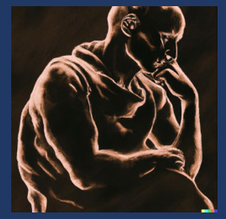
Learning based on Deep Neural Networks



~2010

GENERATIVE AI

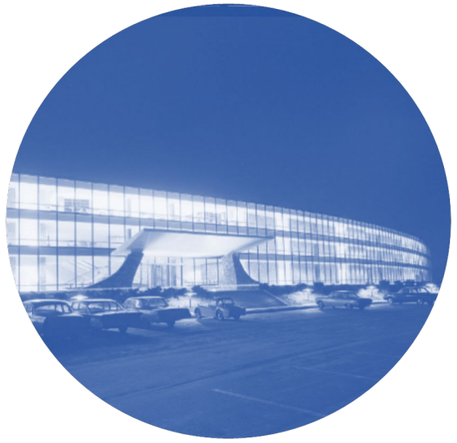
Generates text, images, videos



~2020

High-stakes decision-making applications

Credit



Employment

Admission

Healthcare

Enterprise Workflows

AI Ethics issues -1

Data privacy and governance	AI needs data and can generate data
Fairness	AI can make or recommend decisions, and these should not be discriminatory
Inclusion	Use of AI should not increase the social gaps
Explainability	AI is often opaque
Transparency	More informed use of AI
Accountability	AI is based on statistics and has always a small percentage of error
Social impact	Fast transformation of jobs and society

AI Ethics issues -2

Human and moral agency	AI can profile people and manipulate their preferences
Misinformation	AI can generate plausible but false content
Value alignment	AI can generate harmful content
Environmental impact	Generative AI (foundation models) need huge amounts of energy for training and deployment
Power imbalance	Centralization of data and power

AI Ethics

Multidisciplinary field of study

Main goal: how to optimize AI's beneficial impact while reducing risks and adverse outcomes

Tech solutions: How to design and build AI systems that are aware of the values and principles to be followed in the deployment scenarios

Socio-tech approach: To identify, study, and propose technical and nontechnical solutions for ethics issues arising from the pervasive use of AI in life and society

AI Ethics 3.0

Awareness

- Mostly in academia, multi-disciplinary

2015–2016

Principles

- Corporations, governments, academia, civil society, multi-stakeholder organizations

2017–2018

Practice

- Regulations, standards, corporate directives, processes, auditing, certifications

2019-ongoing

As AI evolves, AI ethics must evolve as well.

Socio-technical issues need socio-technical solutions

- Tools
- Policies
- Education
- Diversity
- Multi-stakeholder consultation

AI Ethics: Every societal actor is involved

Research

- Fairness
- Explainability
- Interpretability
- Robustness
- Privacy
- Value alignment

AI companies

- Governance
- Internal processes
- Tools
- Risk assessment
- Training

Standard bodies

- IEEE P7000 series:
- **IEEE 7000™-2021 – Model Process for Addressing Ethical Concerns During System Design**
- **IEEE P7001™ – Transparency of Autonomous Systems**
- **IEEE P7002™ – Data Privacy Process**
- **IEEE P7003™ – Algorithmic Bias Considerations**
- **IEEE P7004™ – Standard on Child and Student Data Governance**
- **IEEE P7005™ – Standard on Employer Data Governance**
- **IEEE P7007™ – Ontological Standard for Ethically driven Robotics and Automation Systems**
- **IEEE P7008™ – Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems**
- **IEEE P7009™ – Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems**
- **IEEE 7010™-2021 – Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems**
- **IEEE P7011™ – Standard for the Process of Identifying & Rating the Trust-worthiness of News Sources**
- **IEEE P7012™ – Standard for Machine Readable Personal Privacy Terms**

Educational institutions

1. Ethics of AI (University of Helsinki)
2. AI-Ethics: Global Perspectives (aiethicscourse.org)
3. AI Ethics for Business (Seattle University)
4. Bias and Discrimination in AI (Université de Montréal)
5. Data Science Ethics (University of Michigan)
6. Intro to AI Ethics (Kaggle)
7. Ethics in AI and Data Science (LFS112x)
8. Practical Data Ethics (Fast AI)
9. Data Ethics, AI and Responsible Innovation (University of Edinburgh)
10. Identify guiding principles for responsible AI (Microsoft)
11. Human-Computer Interaction III: Ethics, Needfinding & Prototyping (Georgia Tech)
12. Ethics in Action (SDGAcademyX)
13. Explainable Machine Learning with LIME and H2O in R (Coursera)
14. An introduction to explainable AI, and why we need it

ursera)

Governments

AI Bill of Rights (US)
AI Act (EU)
AIDA (Canada)
… many others

Together with: civil society organizations, media, activists, society at large

Nerd for Tech, 2021

Why should organizations that build or use AI care about ethics?

- Company values
- Company reputation
- Social justice and equity
- Client & investor inquiries
- Clients' trust
- Business opportunities
- Existing or expected regulations

IBM Principles for Trust and Transparency

1

The purpose of AI is to augment — not replace — human intelligence

2

Data and insights belong to their creator

3

New technology, including AI systems, must be transparent and explainable

IBM Pillars of Trustworthy AI

Explainability

An AI system's ability to provide a human-interpretable explanation for its predictions and insights

Fairness

Equitable treatment of individuals or groups by an AI system

Depends on the context in which the AI system is used

Robustness

An AI system's ability to effectively handle exceptional conditions, such as abnormalities in input

Transparency

An AI system's ability to include and share information on how it has been designed and developed

Privacy

An AI system's ability to prioritize and safeguard consumers' privacy and data rights

IBM trustworthy AI toolkits

AI Explainability 360
Comprehensive open-source toolkit for explaining ML models & data.

AI Fairness 360
Comprehensive open-source toolkit for detecting & mitigating bias in ML models.

Adversarial Robustness 360
Comprehensive open-source toolkit for defending AI from attacks.

AI Factsheets 360
Extensive website describing research efforts to foster trust in AI by increasing transparency and enabling governance.

AI Privacy 360
Toolbox to support the assessment of privacy risks of AI-based solutions, and to help them adhere to any relevant privacy requirements.

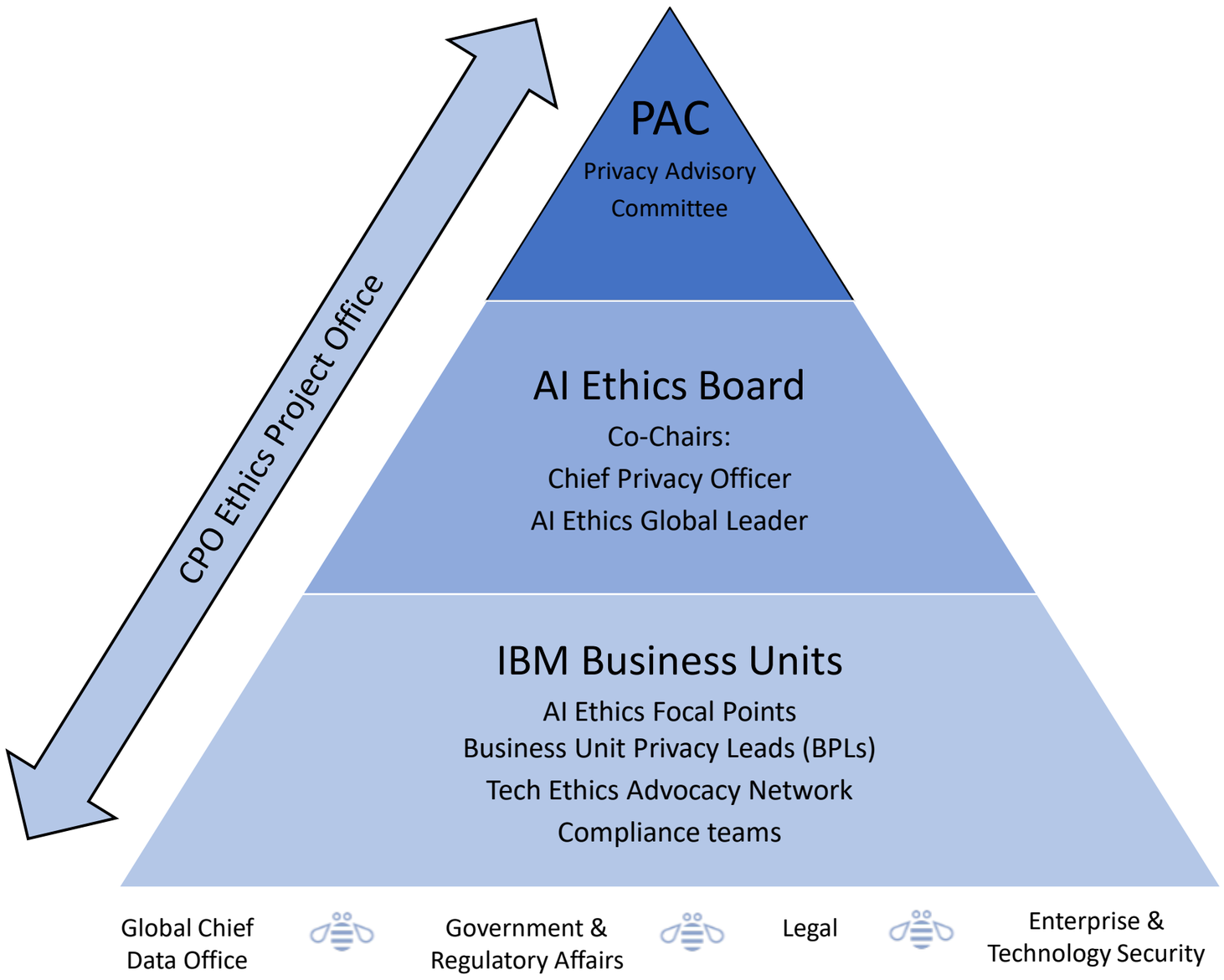
Uncertainty Quantification 360
Comprehensive open-source toolkit for computing and communicating meaningful limitations of ML predictions.

Causal Inference 360
Extensible open-source toolkit for estimating, communicating, and using uncertainty in ML model predictions.

Governance structure

The AI Ethics board is central, cross-disciplinary body to instill a culture of ethical and responsible technology throughout IBM.

The Board's mission is to support a centralized governance, review, and decision-making process for IBM ethics policies, practices, communications, research, products and services.



AI ethics board focus areas

Tech Ethics by Design

- Integrating AI ethics in the technology development pipeline

Use case reviews

- Assessing alignment with Ai ethics principles

Regulation readiness

Education

Amplification and benchmarking

Foundation models

Neurotech

Augmenting Human Intelligence

Multi-stakeholder collaborations

U.S. National AI Advisory Committed (NAIAC)

—

Chief Privacy Officer Christina Montgomery named to NAIAC and U.S. Chamber of Commerce Commission on Competition, Inclusion and Innovation

Partnership on AI

—

Brings together diverse global voices to define best practices for beneficial AI

IBM is a founding member

World Economic Forum's Global AI Action Alliance

—

Guides the responsible development of AI

Co-chaired by Arvind Krishna, IBM Chairman and CEO

MIT-IBM Watson AI Lab

—

Research focused on healthcare, security and finance using the IBM Cloud, AI platform, blockchain and quantum

European Commission Expert Group on AI

—

Defined the ethics guidelines for trustworthy AI

IEEE Global Initiative on AI Ethics

—

Ensures that AI is developed in a way that prioritizes ethical considerations

ITU AI for Good Global Summit

—

Global and inclusive United Nations platform on using AI to achieve the UN Sustainable Development Goals

Data & Trust Alliance

—

Develops new practices and tools to advance the responsible use of data and AI across industries and disciplines

Lessons learnt in operationalizing AI ethics principles

Company-wide approach, not just a team

A governance body, with the power to make decisions for the company

Full operationalization of the principles

Beyond technical tools: also processes, education, risk assessment, and governance

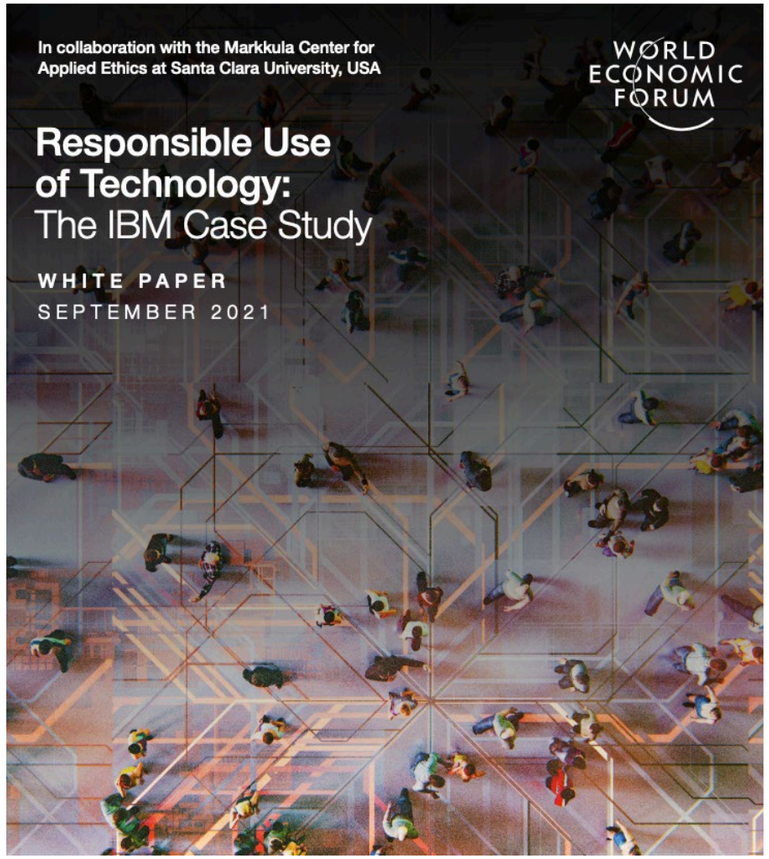
Regulations: beyond compliance

Multi-stakeholder partnerships: to learn and to bring experiences/challenges

Aa AI evolves, AI ethics must evolve as well

Thanks!

IBM’s approach to AI Ethics



Emerging Threat: AI Enabled Cyber Attacks

Timothy Gallagher, Managing Director Kroll Cyber Risk

March 22, 2023

Kroll Cyber Risk

3,000+
IR ENGAGEMENTS / YEAR

53,000+
HOURS OF ASSESSMENT & TESTING / YEAR

100+
INDUSTRY CERTIFICATIONS

A SECRET GIANT

550k+
ACTIVELY MONITORED ENDPOINTS

650+
EXPERTS ACROSS 19 COUNTRIES

TRUSTED EXPERTS

PREFERRED VENDOR FOR
60+
CYBER INSURANCE CARRIERS

90+%
CUSTOMER RETENTION RATE

CREST
Information Security Management ISO 27001 Certified
SOC

UNIQUE EXPERIENCE
INTERPOL
EUROPOL

INDUSTRY RECOGNITION

Bloor
NAMED CHAMPION IN 2023 MDR RESEARCH

Gartner
RECOGNIZED AS REPRESENTATIVE VENDOR FOR MDR & DFIR

SC 2022 awards EUROPE WINNER
2021 Computing Security Awards WINNER
CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2021

Timothy Gallagher

Managing Director

Cyber Risk

- Managing Director in the Kroll Cyber Risk practice, based in Washington, DC
- Previously held a Senior Executive role in the FBI Cyber Division and served as Chief of the FBI Financial Crimes Section
- My practice focus is on where Cyber meets Fraud and Governmental Relations

THE WALL STREET JOURNAL.

What Exactly Is Artificial Intelligence, Anyway?

By Ted Greenwald Follow

Updated April 30, 2018 11:24 am ET

- Simulation of human intelligence in machines to think like humans and mimic their actions
- Using a computer to do things that traditionally require human Intelligence
- Anything a computer can do that was formerly a job for a human

Why are we here?

Explosion in the Availability of Artificial Intelligence

ChatGPT went from 1 million users to 100 million users in six weeks

FBI Issues alert on use of AI for criminal cyber and foreign influence operations

FBI Internet Crime Report: Online Scams cost $10 billion in 2022

Partnerships – law enforcement can provide intel, but mitigation is your task

AI Enabled Cyber Attacks Topics for Discussion

Malicious Code Development	**Threat to Markets**
Business Email Compromise (BEC)/Phishing Attacks	**Public Private Partnerships**

Thank You

Questions?

KROLL

For more information, please contact:

Timothy.Gallagher@kroll.com

Visit kroll.com/cyber

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With 5,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.

© 2022 Kroll, LLC. All rights reserved.

CFTC

COMMODITY FUTURES TRADING COMMISSION

Closing Remarks