digital currency initiative

mit media lab

UnB

MIT Digital Currency Initiative and the University of Brasilia present

# Cryptocurrency Design and Engineering

Lecture 21: Open Source, Money Movement & Privacy: Legal Risks for Developers

Taught by: Amanda Tuminelli and Michael Mosier
Date: December 2, 2025
MAS.S62

*Section 1*

# Why does this topic matter in your studies?

# The Reality: Where You’re Building

**By The Numbers**

- Crypto in 2024: $10.6T volume, $45B illicit = 0.4% illicit
- Traditional finance: 2-5% of GDP ($800B-$2T) = 2-5% illicit

**But…**

Prosecutors/regulators and policymakers are generally applying **laws written for traditional finance**, resulting in collateral impact and uncertainty.

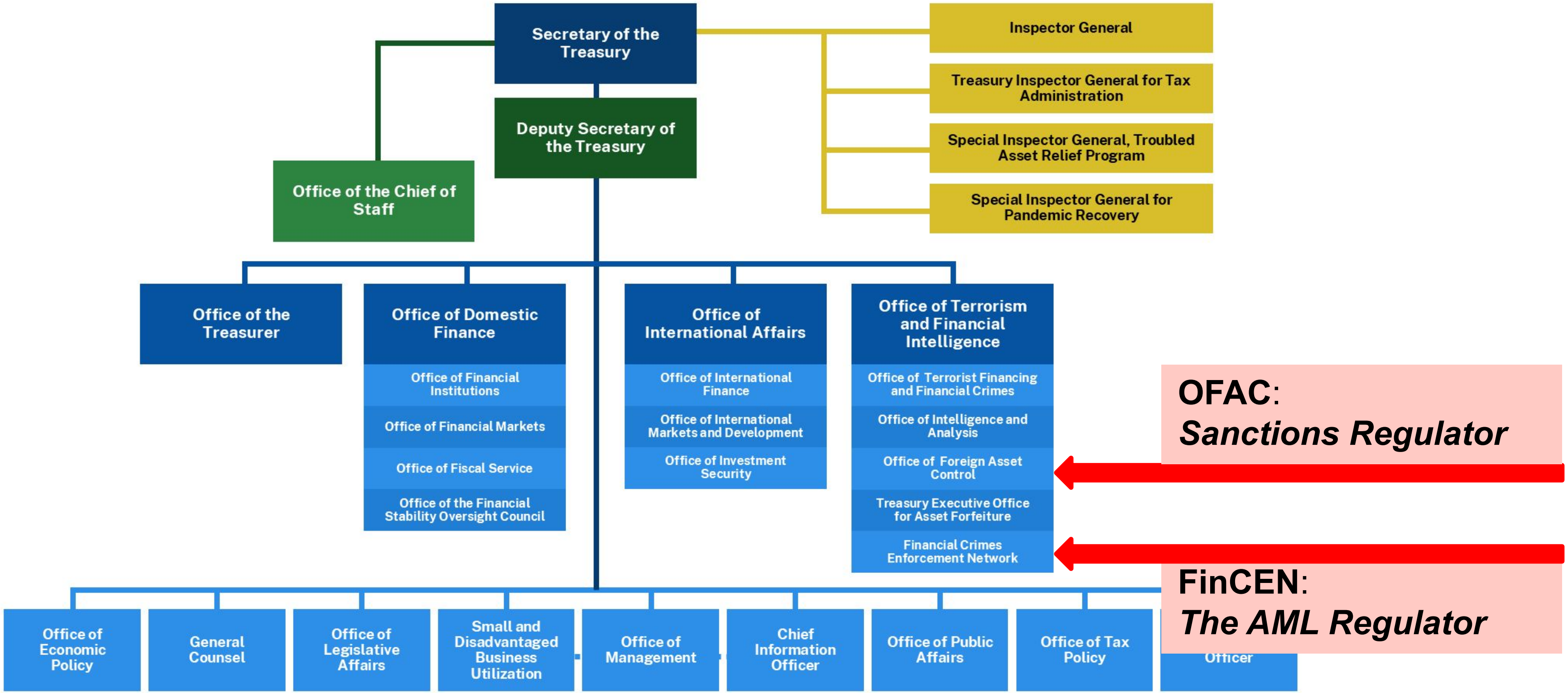
**Today’s goal**

Help you think through the current, evolving landscape.

*Section 2*

# How Does U.S. Government Handle AML and Sanctions?

# U.S. Department of Treasury: An Overview



Secretary of the Treasury

Deputy Secretary of the Treasury

Office of the Chief of Staff

Inspector General

Treasury Inspector General for Tax Administration

Special Inspector General, Troubled Asset Relief Program

Special Inspector General for Pandemic Recovery

Office of the Treasurer

Office of Domestic Finance
- Office of Financial Institutions
- Office of Financial Markets
- Office of Fiscal Service
- Office of the Financial Stability Oversight Council

Office of International Affairs
- Office of International Finance
- Office of International Markets and Development
- Office of Investment Security

Office of Terrorism and Financial Intelligence
- Office of Terrorist Financing and Financial Crimes
- Office of Intelligence and Analysis
- Office of Foreign Asset Control
- Treasury Executive Office for Asset Forfeiture
- Financial Crimes Enforcement Network

Office of Economic Policy

General Counsel

Office of Legislative Affairs

Small and Disadvantaged Business Utilization

Office of Management

Chief Information Officer

Office of Public Affairs

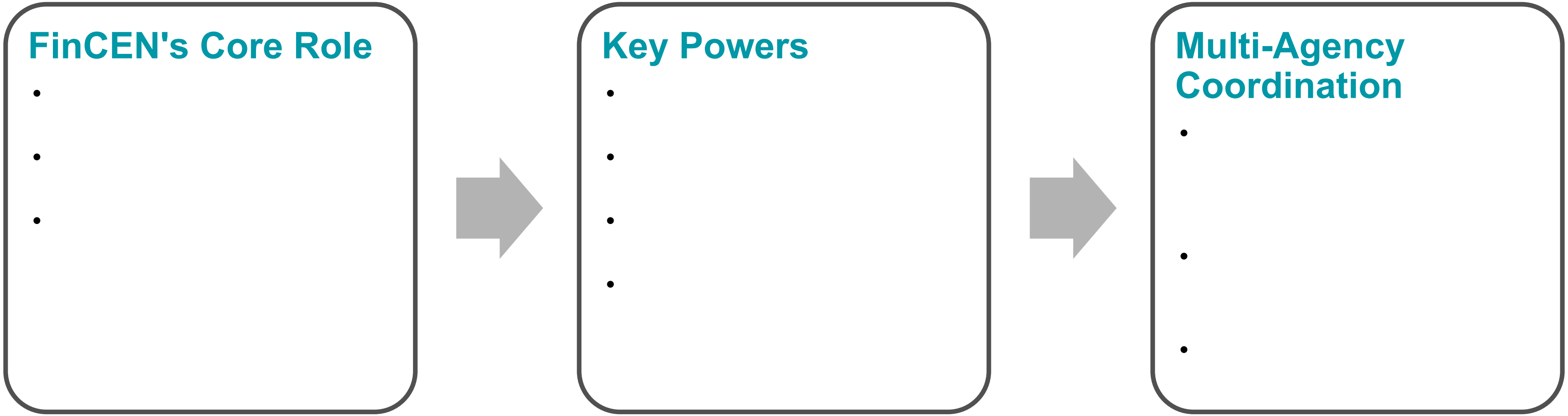
Office of Tax Policy

Officer

**OFAC**:
***Sanctions Regulator***

**FinCEN**:
***The AML Regulator***

# FinCEN: An Overview



### FinCEN's Core Role

- 
- 
-

### Key Powers

- 
- 
- 
-

### Multi-Agency Coordination

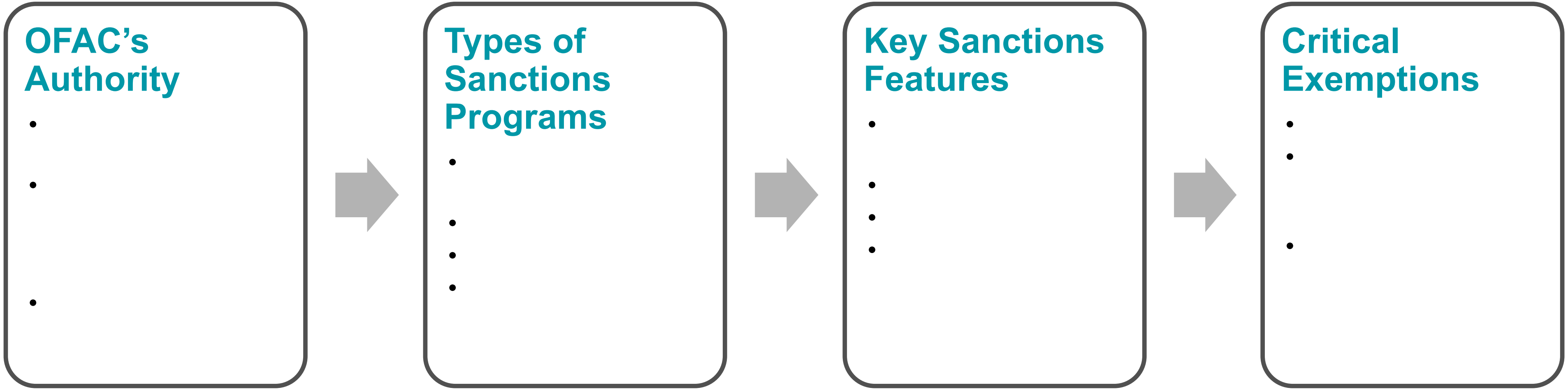
- 
- 
-

## SPOTLIGHTS

**Recent Evolution: Anti-Money Laundering Act (AMLA) 2020**

**2019 FinCEN Guidance**

# OFAC: An Overview



OFAC's Authority

Types of Sanctions Programs

Key Sanctions Features

Critical Exemptions

SPOTLIGHT

**OFAC Virtual Currency Guidance (October 2021)**

# U.S. Department of Justice: An Overview

## DOJ’s Role in AML Enforcement

- Criminal prosecution authority under federal money laundering (Sec. 1956, 1957), money transmitting (Sec. 1960), and conspiracy (Sec. 371) statutes
- Works closely with FinCEN, FBI, IRS-CI, and other law enforcement agencies
- Prosecutes individuals and entities for BSA violations

# DOJ: Key Criminal Statues

## SPOTLIGHTS

### 18 U.S.C. § 1960

- *Operating an unlicensed money transmitting business*

### 18 U.S.C. § 1956

- *Money laundering*

### 18 U.S.C. § 1957

- *Engaging in monetary transactions in property derived from specified unlawful activity*

### 18 U.S.C. § 371

- *Conspiracy to commit offense or to defraud the United States*

***Important Implications for Developers:*** ***Will you be held criminally liable for building technology?***

*Section 3*

# What are key considerations of the Bank Secrecy Act?

# Bank Secrecy Act (BSA): An Overview

Enacted in 1970, the BSA was created to combat money laundering and financial crimes by **requiring "financial institutions" to collect, maintain, and report** certain records.

### Customer Identification Program (CIP)

- Collect customer information, including government ID verification

### Customer Due Diligence (CDD)

- Source of funds, transaction monitoring

### File Suspicious Activity Reports (SARs)

- For transactions $5K+ with "known or suspected" criminal activity & Currency Transaction Reports (CTRs)

### Recordkeeping

- 5-year retention of all records

### Independent Audit

- Annual testing of your AML program

BSA Violations □ Civil or Criminal Penalties

# Bank Secrecy Act (BSA): Compliance Costs

## NOT-SO-HIDDEN COSTS OF BSA COMPLIANCE

### Initial Setup Costs

- *$500K – $1M*

- *Federal FinCEN registration*
- *50+ state MSB licenses (each requires separate application)*
- *Compliance infrastructure*
- *Legal counsel*
- *Blockchain analytics tools*

### Ongoing Annual Costs [medium size]

- *$1M – $5M*

- *All prior, plus…*
- *Compliance officer + team*
- *KYC/AML software subscriptions*
- *Suspicious Activity Report (SAR) filing*
- *Independent audits*
- *Legal fees*
- *Blockchain monitoring tools*

*Section 4*

# Is your innovation custodial or non-custodial?

# Custodial vs. Non-Custodial: The Most Important Technical Distinction

***Key consideration:** determining whether you're a regulated money transmitter*

| | CUSTODIAL | NON-CUSTODIAL |
|---|---|---|
| *Technical Characteristics* | • Entity holds users' private keys<br>• Entity can execute transactions without user signatures<br>• Entity can freeze, reverse, or prevent transactions<br>• Users can't withdraw without permission | • Users hold their own private keys and sign transactions<br>• No one can prevent users from transacting<br>• Software may facilitate, but doesn't control funds or transactions<br>• No ability to freeze or reverse |
| *Examples* | • Coinbase, Kraken, Binance (centralized exchanges)<br>• Custodial wallet providers<br>• Traditional escrow services | • MetaMask, Rainbow Wallet (self-custody wallets)<br>• Uniswap protocol (decentralized exchange)<br>• Hardware wallets<br>• Tornado Cash immutable contracts |
| *Legal Status* | **Clearly regulated as MSB:**<br>• Must register with FinCEN<br>• State-by-state MSB licenses required<br>• Full KYC/AML programs mandatory<br>• Suspicious Activity Reports (SARs)<br>• Can cost millions per year in compliance | **Historically NOT regulated as MSBs (per 2019 FinCEN Guidance):**<br>• "Software providers" explicitly exempt<br>• Providers of "communication or network access services" exempt<br>• BUT: recent cases suggest this may be changing |

*Section 5*

# Why is ‘privacy’ technically necessary in tech builds?

# Privacy: Why It’s Technically Necessary

## Blockchain’s Privacy Problem

*Every blockchain transaction is…*

- * Publicly visible forever*
- * Permanently linked to your address*
- * Traceable across all your activity*

*… Like publishing your bank statements, credit card bills, and investment portfolio on a public website.*

## Legitimate Privacy Use Cases

- * Individual Privacy*
- * Business Privacy*
- * Safey and Civil Society Privacy*

## Technical Solutions

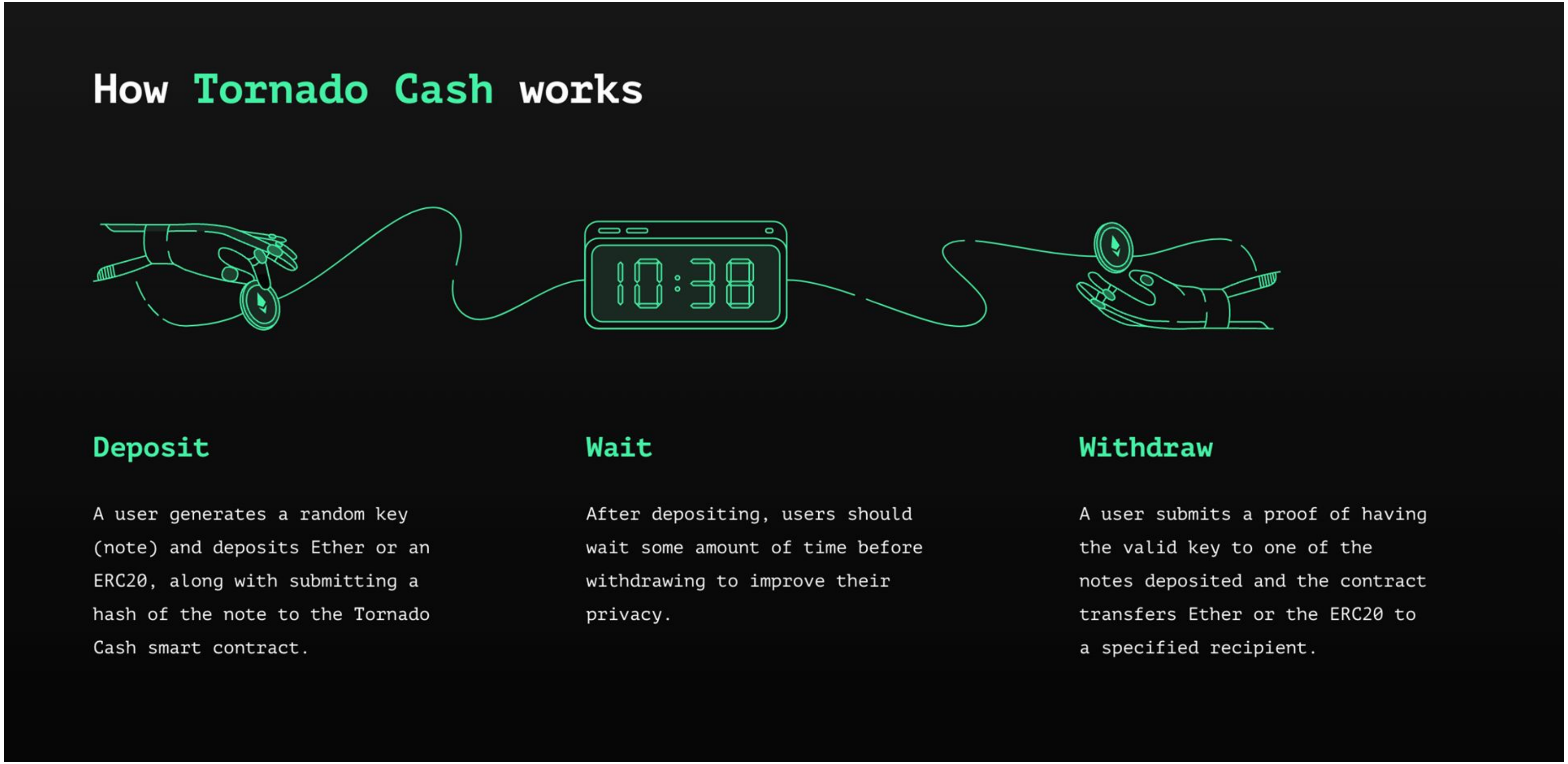
- * Privacy services (Privacy Pools)*
- * Privacy coins (Zcash)*
- * Zero-knowledge proofs-based networks (Aleo)*
- * Stealth addresses*

***Dual-Use Dilemma*: Like many tools, privacy tech can be used by both legitimate and criminal actors**

*Section 6: Case Study*

# What happened to Tornado Cash developers?

# Tornado Cash: An Overview



## How Tornado Cash works

### Deposit

A user generates a random key (note) and deposits Ether or an ERC20, along with submitting a hash of the note to the Tornado Cash smart contract.

### Wait

After depositing, users should wait some amount of time before withdrawing to improve their privacy.

### Withdraw

A user submits a proof of having the valid key to one of the notes deposited and the contract transfers Ether or the ERC20 to a specified recipient.

# Tornado Cash: Government Actions

### OFAC Sanctions (Aug 2022)

Office of Foreign Assets Control added Tornado Cash smart contract addresses and website to SDN List

### Van Loon v. Treasury: Fifth Circuit (Nov 2024)

Individual Tornado Cash users sued the Treasury Department, alleging that OFAC’s sanctions were illegal

### U.S. v. Storm and Semenov: Criminal Prosecution (Ongoing)

Roman Storm and Roman Semenov, two of three Tornado Cash co-founders, were charged in August 2023, accused of 1) Conspiracy to operate unlicensed money transmitting business (§ 1960); 2) Conspiracy to commit money laundering; 3) Conspiracy to violate sanctions (IEEPA)

# Tornado Cash: Roman Semenov and New “Contributor” Sanctions Problem

**Who**: Roman Semenov, Tornado Cash co-founder

**Status**: Added to OFAC SDN List (November 2022) and he remains sanctioned today

**The Problem**:

- His code was delisted (Van Loon case), but HE is still sanctioned as an individual "contributor"
- No clear standard for what makes you a sanctionable "contributor"

**Unanswered Questions for Developers**:

- What level of contribution triggers this?
- How do you get delisted if you have no control to "change behavior"?
- Does contributing to open-source protocols make you personally liable for downstream use?

*Section 7*

# Can we compare Tornado Cash and Samourai Wallet?

# Samourai Wallet: An Overview

***Samourai Wallet* is an *unhosted wallet provider and privacy "service"* built on the Bitcoin blockchain**

### Who?

Two developers of Samourai Wallet, Keonne Rodriguez and William Lonergan Hill

### The Charges

- Operating an unlicensed money transmitting business (§ 1960)
- Conspiring to commit money laundering

### The Government's Theory

The DOJ charged the developers of Samourai Wallet based on:

- *Providing "whirlpool" mixing, a coinjoin that obfuscated the source of cryptocurrency transactions*
- *Operating a centralized server*
- *Taking fees from the "service"*
- *Continuing to operate while knowing criminals were using Samourai Wallet*

# Samourai Wallet vs. Tornado Cash

| | Tornado Cash<br>(Roman Storm) | Samourai Wallet<br>(Rodriguez & Hill) |
|---|---|---|
| *Technology* | • Immutable smart contracts on Ethereum | • Centralized coordination server on Bitcoin |
| *UI* | • Provided widely used UI | • Provided widely used UI |
| *Fees* | • Took fees | • Took fees |
| *Knowledge of Criminal Activity* | • Knew about criminal activity | • Knew about criminal activity; explicitly marketed to criminals |
| *Outcome* | • Pled not guilty, went to trial, and convicted on § 1960 (unlicensed MSB) – awaiting sentencing | • Both pled guilty on § 1960 charge in August 2025 |

***Open Question:** Does the fact that Samourai Wallet was built on Bitcoin and with a centralized coordination server change the "control" analysis?*

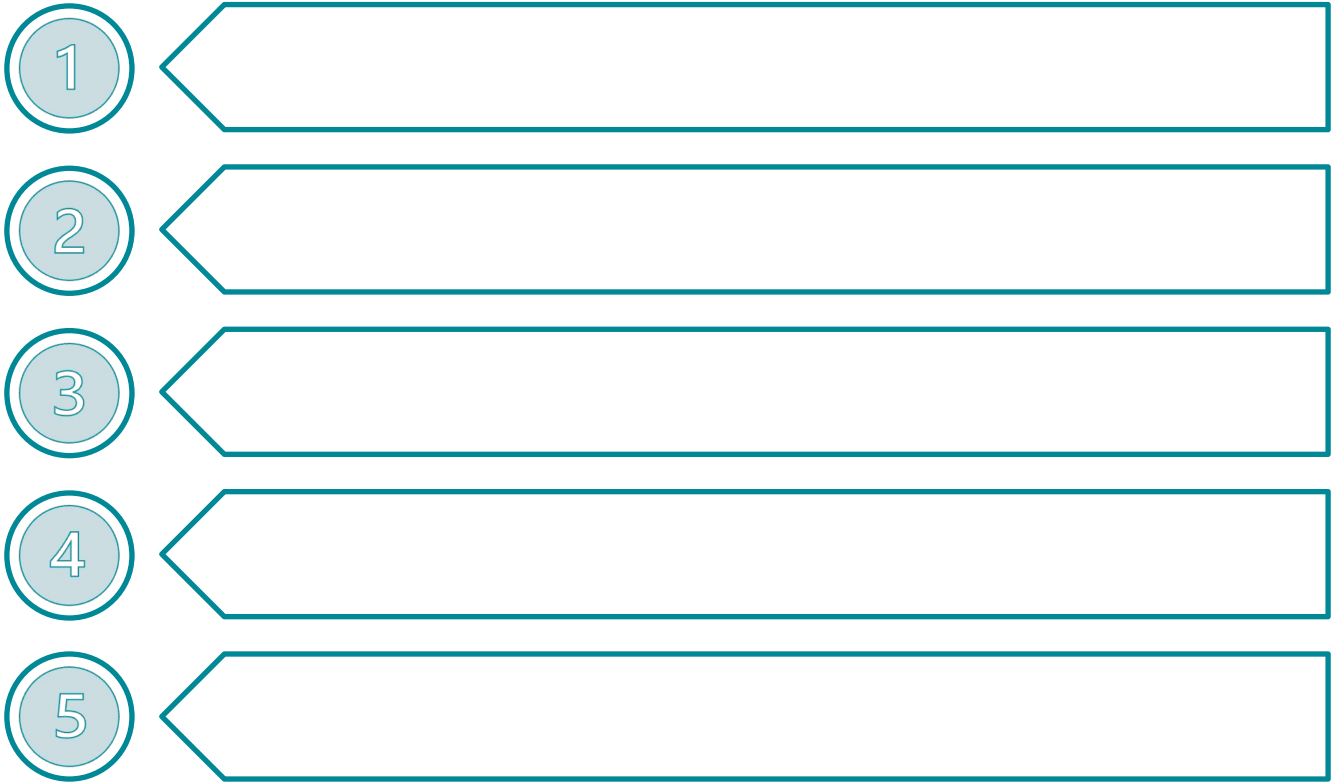
# Samourai Wallet vs. Tornado Cash

***Big Takeaway:*** ***Tech architecture matters, but so does control, custody, and conduct***

*Section 9*

# What are today's unanswered legal questions?

# Unanswered Legal Questions: An Overview



# Unanswered Legal Questions: Potential Clarifications Forthcoming

## Congressional Action

## New FinCEN Guidance

## Court Actions

# Building Blockchain: Recap & Look Ahead

**You're building in a space where:**

- Technology evolves faster than law and regulations
- Courts are figuring this out as they go
- Developers are bearing risk

**The optimistic view:**

- Crypto is 10x cleaner than traditional finance
- Technology enables far more transparency than in TradFi, but exposure creates personal risk for users that needs to be mitigated
- Privacy is solvable with better design
- Law will eventually catch up, and do so accurately if we help educate policymakers
- But we're in the messy transition period

***Thank you so much for doing the important work of building our future.***

*Questions? Want to continue the conversation?*

**Amanda Tuminelli**
tuminelli@defieducationfund.org

**Michael Mosier**
mm@arktouros.co

**FIN.**

# Architecture Risk Spectrum: An Overview

## Lowest Risk

- Pure software tool, released and walk away
- Users hold their own keys (non-custodial)
- True peer-to-peer, no intermediation
- No fees to developers
- No ongoing involvement

**Example:** Release a wallet library on GitHub

## Medium Risk

- Deploy autonomous smart contracts
- Provide UI that users access
- Take fees or make money
- Do ongoing updates/improvements
- Market the tool
- Substantial DAO governance participation

**Example:** DeFi protocol development

## Higher Risk

- Hold users' private keys (custodial)
- Can freeze or reverse transactions
- Centralized servers coordinate transactions
- Provide customer support
- Control access to the system

**Example:** Any custodial exchange or service

# Developer Takeaways: An Overview

| | REMINDERS FOR SOFTWARE DEVELOPERS |
|---|---|
| *1* | The traditional bright line is custody & control |
| *2* | “I just wrote code” is not a legal defense |
| *3* | Immutable smart contracts can’t be sanctioned, but people can be |
| *4* | Privacy is legitimate and technically necessary |
| *5* | The costs of ‘getting it wrong’ are meaningful |
| *6* | Tech architecture decisions matter, and so does intent |
| *7* | Seek legal counsel before deploying |
| *8* | The law is evolving in real-time |