# Structuring Censorship Resistant Privacy Protocols: Risks and Considerations

Amal Ibraymi

Andre Omietanski

Fatemeh Fannizadeh

Part I

# Introduction

# Agenda

01 Introduction

02 Assessing Risks

03 Life Cycle of a Protocol (Breakout Session)

04 Some Considerations

05 Discussion

# Disclaimer

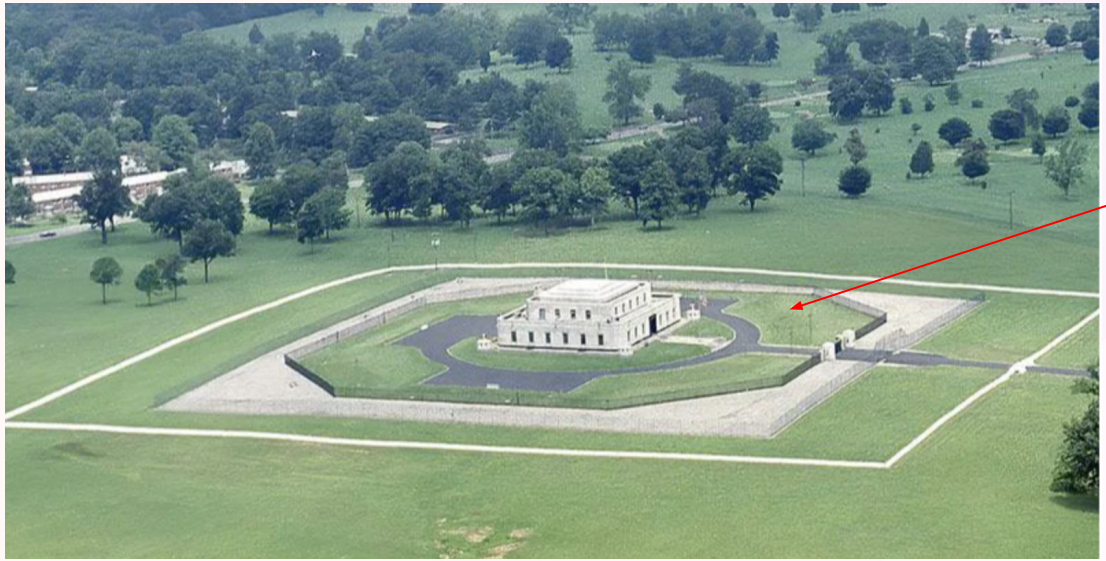
- This workshop does not constitute **legal advice**.
- This workshop does not give rise to any **attorney/client relationship**.
- The contents of this presentation are for general information purposes only.
- Always seek your **own** specialist legal advice.


Each project is different; do your own research / hire your own lawyer!

- There is significant uncertainty/confusion in the industry
- No clear laws
- *Political enforcement actions* in the US

- Building privacy focused protocols is currently contrarian
- General crypto regulatory environment is likely to shift post Trump victory

# Building involves legal structuring



# Why are you here?

Part II

# Assessing Risks

# How to approach thinking about risks

### Regulatory Overview

Understand the existing legal regulatory framework and its impact on privacy protocols

### Stakeholder-Specific Risks

Understand the risks associated with each stakeholder

### Phase-Specific Risks

Identify the **certain main risks** at each stage of the protocol development

# Regulatory Overview

# US Sanctions

- Applies to U.S. citizens/entities, prohibiting dealings with sanctioned individuals/entities
- Transactions involving blocked addresses or blacklisted individuals/entities could trigger enforcement

# US Bank Secrecy Act / Money Transmission Laws

- The Bank Secrecy Act (BSA) requires money service businesses to register with FinCEN and perform certain compliance obligations such as KYC/AML checks
- Money transmission defined as accepting and transmitting currency or value (with exceptions).
- These requirements are enforced civilly by FinCEN and criminally by the Department of Justice.

# EU MiCA

- Applies to crypto-assets service providers in the EU. Carve out for *"crypto-asset services…provided in a fully decentralised manner without any intermediary…"*
- No definition of "fully decentralised" has been proposed or exists
- Covers issuance, trading, and custody of crypto-assets, with requirements for transparency and consumer protections.

# US Securities laws

- U.S. Securities and Exchange Commission (SEC) uses the Howey Test to determine whether an asset is a security
- If a protocol’s tokens are deemed securities, they may have to comply with registration and disclosure requirements

Part III

# Life Cycle of Protocol Development

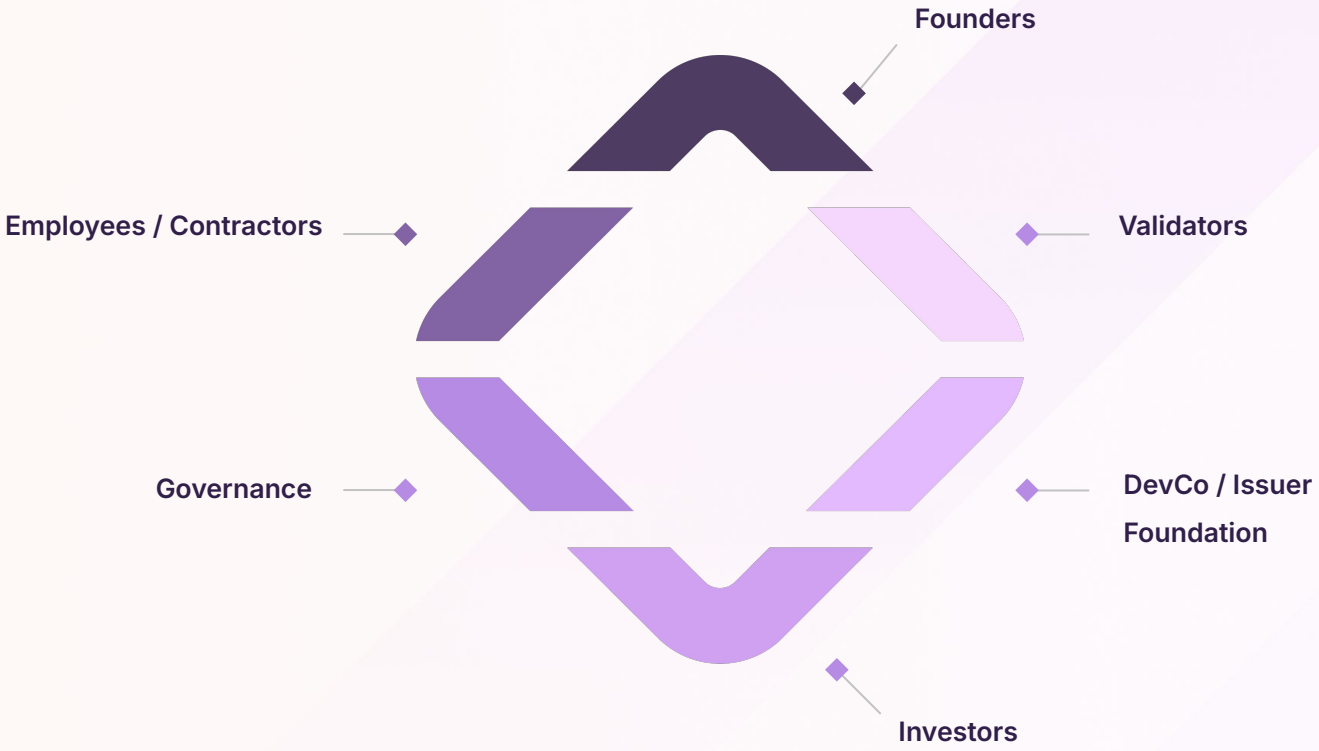
# Early Life Cycle of Protocol Development

Stakeholder involvement changes throughout the life cycle, impacting their exposure.

**Legal / practical risks need to be considered throughout the protocol lifecycle.**

1. **Development Stage**
2. **Prelaunch**
3. **Launch/Early Operations**

# Certain Stakeholders



# Breakout Session - 20 mins

**Question**: What are the risks associated with each stakeholder?

**Task**: Mark **High**, **Medium**, **Low** and specify lifecycle phase

# Risk Matrix - Overly Simplified Overview

| | | Sanctions | AML / KYC | Securities |
|---|---|---|---|---|
| Stakeholders | Founders | | | |
| | Validators | | | |
| | Node Operators | | | |
| | Core Developers | | | |
| | Token | | | |
| | Governance | | | |
| | Employees | | | |
| | DevCo / Issuer | | | |

# Assumptions

### Founders

- 2 co-founders:
  - one based in France
  - one based in the US

### Employees / Contractors

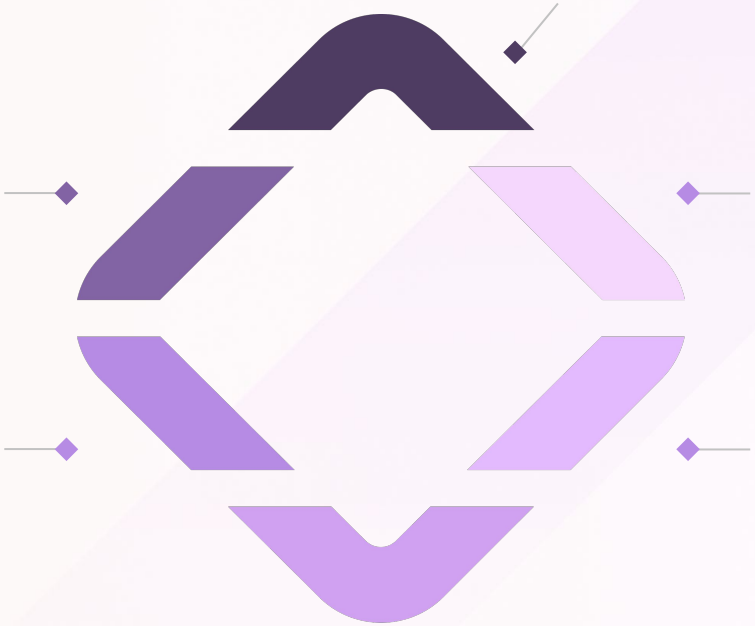
- 51% at DevCo based in the US
- 1 core developer in the Netherlands

### Validators

- 16 Genesis Validators - 30% are US centralised exchanges

### Governance

- DAO Token voting
- 5 member security council upgrade multi-sig:
  - anonymous,
  - 3 DevCo employees on multi-sig
- Foundation holds 50% of token supply at mainnet launch, but intends to give out grants asap
- Founders collectively hold 20% of supply



### DevCo / Issuer / Foundation

- BVI issuer / mainnet deployer with full protocol functionality
- Panama Foundation gives grants to incentives US validators to join
- DevCo is developing centralised interface to access protocol shielding

### Token

- ICO public sale to world
- Airdrop announced at testnet

Part IV

# Some Considerations

# Scope of Project & Control / Jurisdiction

- **Decentralise.** Decentralise, decentralise, decentralise

  💡: ensure no entity group or collective of connected individuals owns a % token supply that can imply control.

  💡: emergency halt only (for technical bugs) > upgrade mult-sigs. Non-anonymous multi-sigs may be better optically.

- **Issuer Entity**. Consider launching your project (and token (if any)) from crypto-friendly jurisdictions and through a non-profit entity.

  💡: Switzerland non-profits have been used for privacy projects. Switzerland Foundation > Panama Foundation

# External Messaging /Marketing

- **Alignment**

  💡:Ensure all external messaging (website, social media, marketing) aligns and doesn't imply any control (direct / indirect) over decentralized aspects of the protocol.

- **Privacy vs. Anonymity**

  💡:Emphasize privacy-enhancing features in your messaging, NOT as enabling "anonymous transactions".

- **Labs vs. Foundation**

  💡:Don't confuse the roles of a Labs entity and a Foundation

- **Token & Airdrop**

  💡:Don't mention / preview any airdrop or token (prior to mainnet / launch)

  💡:Tokens ≠ investments

# Develop Sanctions Compliance Tooling

- **No in-protocol compliance checks are currently expressly required by statutes / acts of law**, in particular for decentralised protocols.
- **Our personal view remains that decentralised protocols should be neutral and no backdoors implemented**.
- However, to empower / remove “builders angst” for developers building on your protocol, consider providing best practices / tooling for them to implement at their option**:**
  - **Sanctions Compliance**

    💡**:** Give access to ZK “Proof of Innocence” tooling (but not require usage) (On-Chain Sanctions Compliance)

    💡**:** Give access to ZK “Proof of Passport” tooling (but not require usage) (Off-Chain Sanctions Compliance)

# General

- **Terms & Conditions (T&Cs) and Privacy Policy**

  💡:If your protocol has a testnet / incentives / points, ensure you have clearly defined T&Cs and a Privacy Policy that comply with applicable laws

- **Get Legal Advice**

  💡:Hire a lawyer to review your protocol's design early on, governance structure, and responses to key legal questions and ensure ongoing monitoring

- **Intellectual Property**

  💡: Consider protecting the protocol's intellectual property (name / logo) through trademarks

# Key Takeaways

01

## Start Early!

Prepare responses to the questionnaires sent and address potential legal risks early

02

## Decentralise

Well-structured decentralized governance (from launch) may help mitigate liability

03

## Stay ahead of the curve

Laws are always evolving so continuous legal oversight is essential.

Part V

# Discussion

## Top 10 Questions

## Decentralisation Matrix