CFTC

COMMODITY FUTURES TRADING COMMISSION

Technology Advisory Committee Meeting – July 18, 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: Responsible Use of AI in Regulated Financial Services

What capacities, tools, definitions, inputs, resources, etc. are needed to make regulation, self-regulation, liability and other forms of accountability work?

ARTIFICIAL INTELLIGENCE ACCOUNTABILITY POLICY

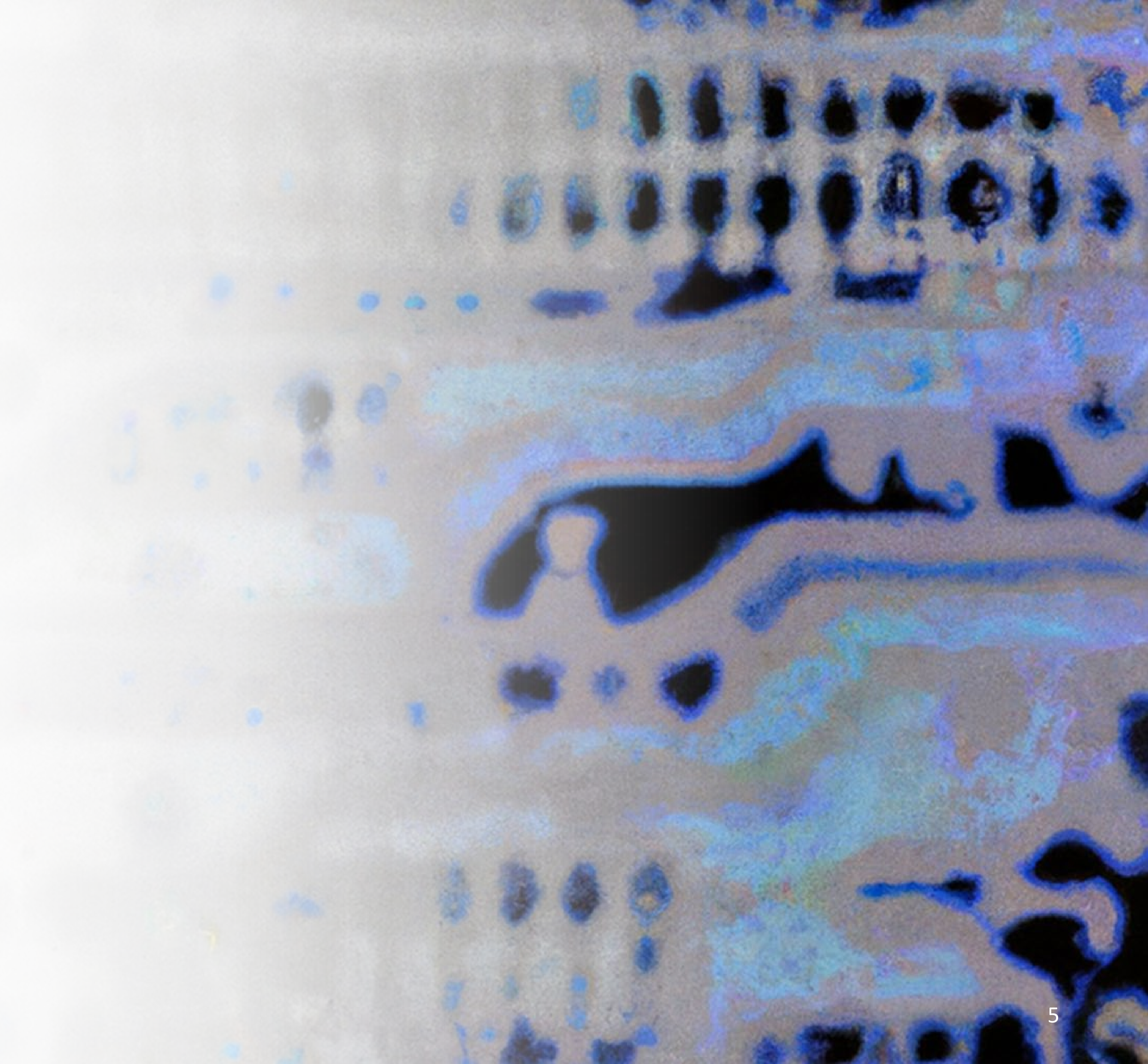
REQUEST FOR COMMENT

AI Accountability Policy

Accountability for “trustworthy” AI systems will entail choices about:
- design and documentation,
- risk allocation and reduction,
- regulation and enforcement.

These activities require tools like certifications, assessments, and audits to show that an AI system is legal, fair, safe & effective, and otherwise trustworthy – a function also known as providing AI assurance.

Policies can promote the development and use of these tools – to foster an AI accountability ecosystem.



34+ questions, for example:

1. Objectives of accountability tools?
   - Verify claims, compliance with legal standards, or with non-binding trustworthy AI goals?
   - Verify particular goals (fairness, safety, transparency and explainability)?
   - Part of cyber, human rights, other accountability efforts?
   - How to address systemic or emergent risk?
   - Measures to prevent audit-washing – providing unreliable assurance?
2. Existing resources and models?
3. Subjects of accountability?
   - Where in the lifecycle? Continuous assurance or for adaptive systems?
   - Where in the value chain? Role of vendors?
   - Special obligations for public procurement?
4. Accountability inputs and reporting?
   - What to do about data quality and voids?
   - What logs, documentation are necessary for adequate assurance, especially by independent auditors or certifiers?
   - Researcher access?
   - Communicating assurance audits, etc?
5. Barriers?
   - Trade secrets and IP?
   - Costs and personnel?
   - Tools and standards?
6. New Policies?
   - Mandatory audits and/or certification?
   - Federal subsidies/support for field?
   - Data access?
   - Disclosure and documentation incentives or requirements?

Report and recommendations: FALL 2023

Possible areas of focus:

- Audits
- Auditor access and independence
- Bounties; distributed tools
- Certifications
- Data sets
- Documentation
- Prizes and support
- Regulation & self-regulation
- Accountability for AI regulatory tools

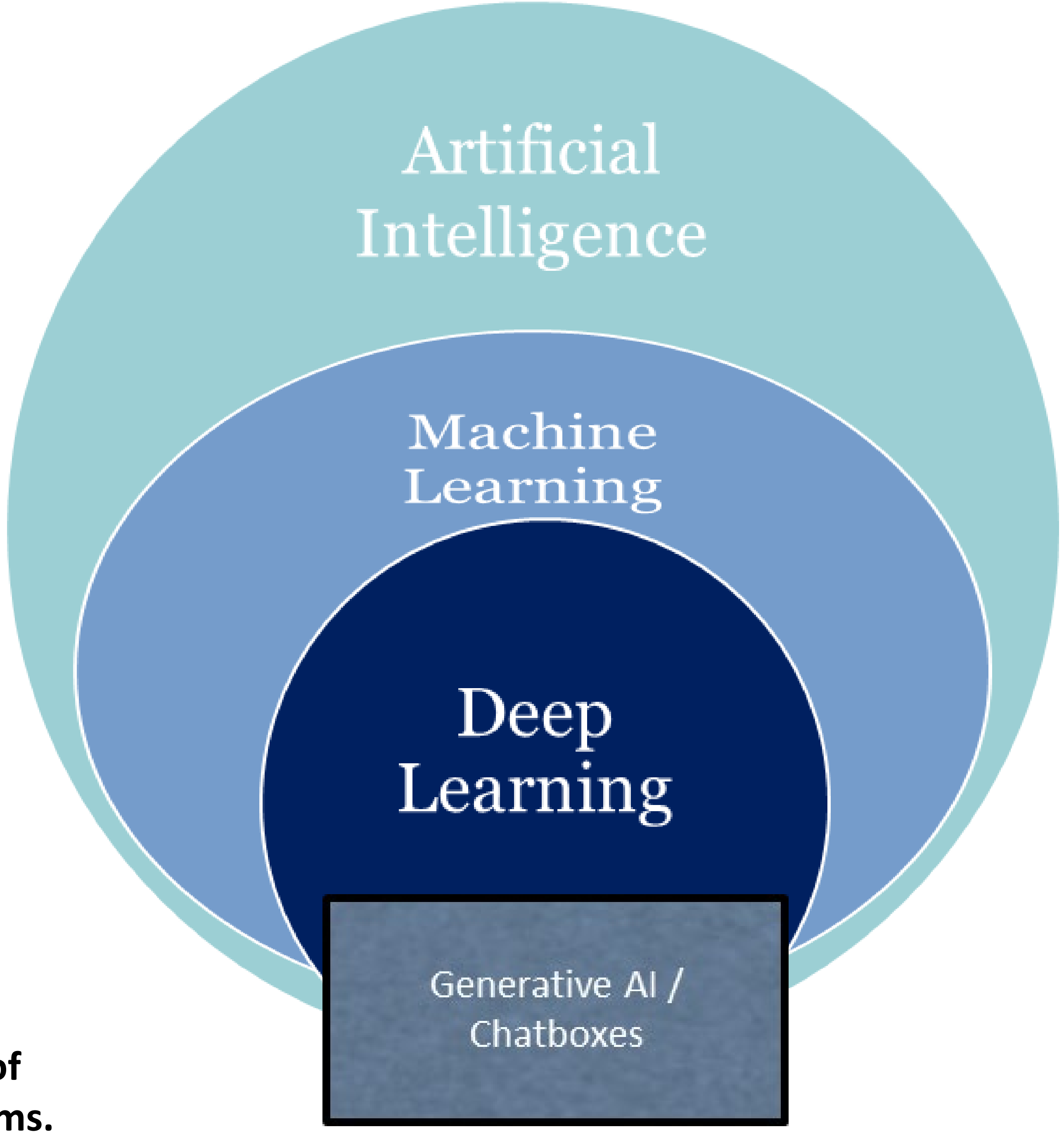
BROOKINGS | QUALITY. INDEPENDENCE. IMPACT.

Responsible Artificial Intelligence (AI)

Nicol Turner Lee, Ph.D.
Senior Fellow and Director, Center for Technology Innovation
The Brookings Institution

July 18, 2023 – Presentation to CFTC

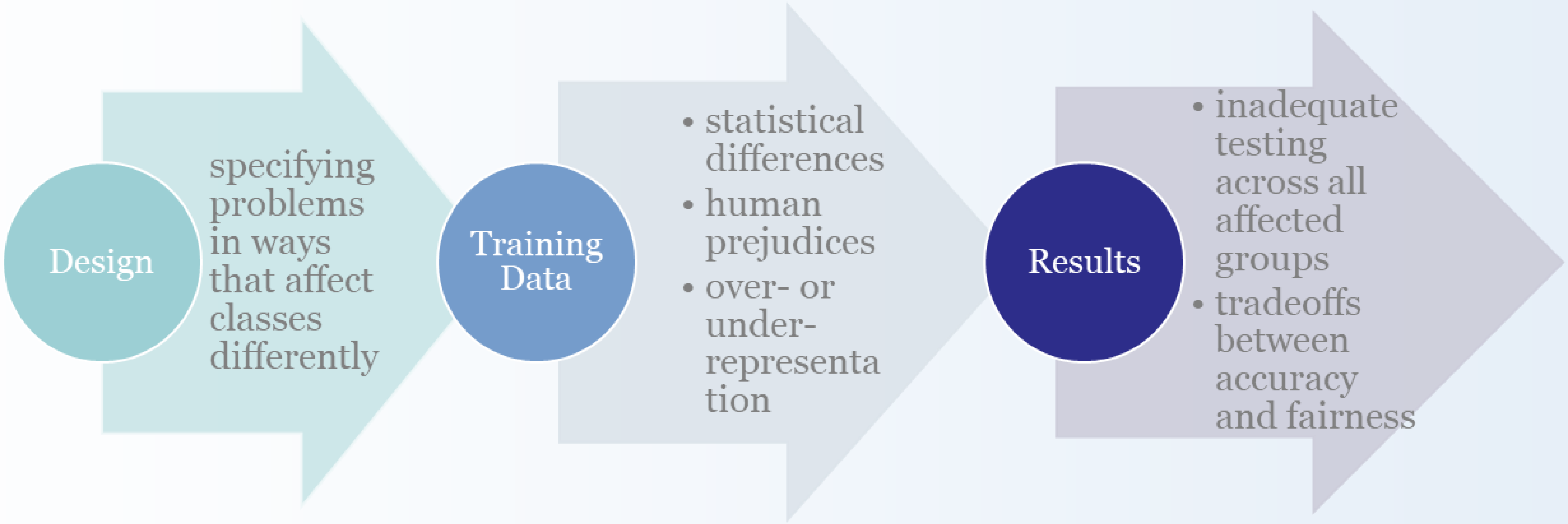
AI: The New Ecology



Taken together, these emerging technologies have the ability to efficiently and quickly solve a host of existing and unforeseen social problems.

Biases and other Challenges at any Stage

Bias can be introduced at any stage of the life cycle of the algorithm



Design
specifying problems in ways that affect classes differently
Training Data
• statistical differences
• human prejudices
• over- or under-representa tion
Results
• inadequate testing across all affected groups
• tradeoffs between accuracy and fairness

Inferences from data about people – including their identities, demographic attributes, preferences, and likely future behaviors – can have adverse impacts on disfavored groups beyond just protected classes.

Training data can be historically and contextually traumatized.

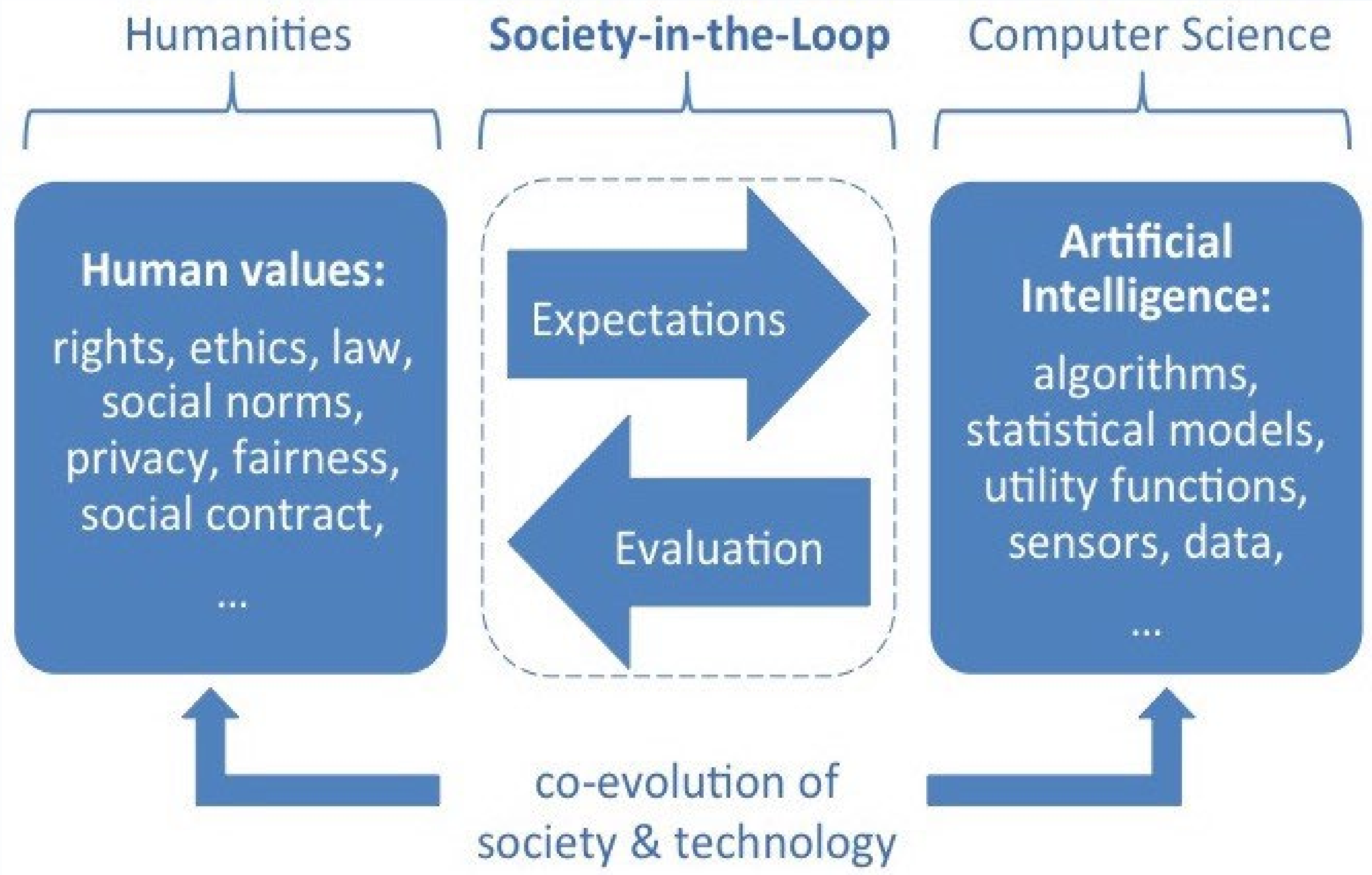
Examples of AI biases

- Ad targeting
- Employment bias (e.g., gender, race, age)
- Facial detection errors and inaccuracies
- Search query misrepresentation
- Criminal justice / predictive policing “big” mistakes
- Credit scoring and other financial services errors
- Political dis- and mis-information
- Health care practices and research

Risks and concerns are socio-technical

- Societal
  - **Biased decision-making:** AI-driven algorithms often contain gender, racial, or other implicit biases that reinforce systemic discrimination.
  - **Deliberate misuse:** malicious actors may spread disinformation, create deepfakes, and conduct unauthorized surveillance or profiling.
  - **And more**: job displacement, data privacy, plagiarism/copyright/IP, carbon emissions & environmental impact of training large models.
- Technical
  - How do we **“operationalize” and measure** abstract values (e.g., fairness)?
  - How should developers approach **trade-offs** (e.g., fairness and accuracy, or privacy and national security)?
  - Given the context-dependent and constantly evolving use cases for AI, how can we **set industry standards** that are robust and scalable?
  - Conflation of AI for **efficiency** and disparate outcomes

Toward more responsible AI from a learning context


Humanities
Society-in-the-Loop
Computer Science
Human values:
rights, ethics, law, social norms, privacy, fairness, social contract,
…
Expectations
Evaluation
Artificial Intelligence:
algorithms, statistical models, utility functions, sensors, data,
…
co-evolution of society & technology

AI in Financial Services/Products: Use Cases

- **Risk Management** – calculate and simulate risks associated with compliance protocols, trading positions, or credit/lending decisions.
- **Fraud Prevention** – identify cases of credit card fraud or money laundering by tracking clients' behavior/buying habits.
- **Algorithmic Trading** – execute trades with a speed, precision, and frequency impossible for human traders.
  - Traders can train algorithms to find patterns in past transactions or monitor real-time market data, identify arbitrage opportunities, and instantaneously place buy/sell orders at the most optimal prices.

Financial algorithms can do all the above. What about generative AI?

- **Engage** with questions from clients or investors.
- **Research** competitors, markets, and consumer sentiment.
- **Draft** contracts, reports, or presentations.

Sources: Algorithmic Trading | Investopedia; Impact of AI on Fintech | Toward Data Science; Business Harness Generative AI | WSJ

Key Challenges in Financial Services & Products

- **Bias mitigation** – bias in, bias out
  - Ensure that training data for AI-driven algorithms is representative, accurate, and values-based.
  - Include diverse communities of “humans-in-the-loop” who clean and label datasets, and train and build AI models.
- **Transparency** – explain the “black box”
  - Explainability of computational models and training datasets
  - Disclosures of application – before, during, and after
  - Privacy of data used to train models to avoid proprietary mining
  - Avoidance of “insider” use to manage risk
- **Regulation** – self-regulatory versus proscriptive

Source: Challenges of AI Regulation | Brookings

Regulatory Landscape

“Soft” law – voluntary self-regulation or opt-in best practices

- Examples: Partnership on AI, EU’s Code of Practice on Disinformation, NIST’s AI Risk Management Framework, OSTP’s Blueprint for an AI Bill of Rights
- **Advantages**:
  - » Promotes innovation, with minimal disruption to business models.
  - » Encourages collaboration and consensus among stakeholders (e.g., tech companies, civil society organizations, policymakers, and academics).
- **Limitations:**
  - » No enforcement mechanisms, so no legal remedies are available for violations.

“Hard” law – enforceable requirements and regulations

- While global actors like the EU or China pass binding legislation, the US faces a regulatory gap, as “hard” law falls behind “soft” law (often faster to implement).
  - » Federal legislation on AI is still pending, and some states have introduced their own bills.
- **Challenges**:
  - » “Hard” law requires bipartisan support to pass.
  - » State and federal agencies need resources to exercise proper oversight.

Source: Soft Law in AI Governance | Brookings; How California and Other States are Tackling AI Legislation | Brookings

Examples from EU Legislation

- Different approaches for different environments (cf. Alex Engler)
- **General Data Protection Regulation (GDPR)**
  - AI needs human supervision to make decisions affecting legal rights.
  - Individual right to “meaningful information about the logic” of an automated system
- **Proposed AI Act: Tiered system**
  - Deepfakes, chatbots, biometric analysis, etc.
    - Mandatory disclosure
  - High Risk: Regulated consumer products and AI used for impactful socioeconomic decisions
    - Standards of data quality, accuracy, and non-discrimination
    - Technical documentation, record-keeping, risk management, and human oversight
  - Unacceptable Risk: AI for social scoring, emotion-detecting FRT
    - Banned
- **Digital Services Act (DSA)**
  - Requires large platforms to explain automated recommendation systems.

Source: The EU and U.S. diverge on AI regulation | Brookings

Current U.S. Policy Proposals

- **The U.S. approach is "risk based, sectorally specific, and highly distributed across federal agencies."**
- **Agencies required to develop AI regulation plans**
  - » Executive Order 13859 (2019) and OMB Guidance M-21-06
  - » Most have not done so
- **Potentially more multistakeholder-focused to improve socio-technical cadence:**
  - » Consumer Financial Protection Bureau (CFPB) requires explanations for credit denials by AI
  - » Food and Drug Administration (FDA) publishes best practices for AI in medical devices
  - » Consumer Products Safety Commission (CPSC) issued a draft report on how to test and evaluate consumer machine learning products
  - » "Energy star rating" multistakeholder practices
- **Discussions on standards and licensing, consumer disclosures**
- **Calls for federal privacy legislation**

Source: The EU and U.S. diverge on AI regulation | Brookings

U.S. Implementation Siloes

- **White House Office of Science and Technology Policy (OSTP): Blueprint for an AI Bill of Rights (AIBoR)**
  - Voluntary roadmap for agencies for responsible AI
  - Articulates five broad principles for mitigating AI harms
- **National Institute of Standards and Technology (NIST): AI Risk Management Framework (RMF)**
  - Voluntary roadmap for developing responsible AI
  - Offers comprehensive suggestions for mitigating risk throughout the AI lifecycle

Source: The EU and U.S. diverge on AI regulation | Brookings; Opportunities and blind spots in the White House's blueprint for an AI Bill of Rights | Brookings

What’s needed

- **Less segmentation and more clarity over jurisdictional authority in the U.S.** – Where should authority be placed, or should it be more distributed?
- **Potential harmonization with EU regulation** – What’s worthwhile to explore?
- **Sectoral regulations** – How should existing regulation and best practices be integrated into discussions?
- **Emerging technologies** – What about the use and regulation of generative AI?
- **Self-regulation** – With current calls from industry, should we trust voluntary commitments as the next viable option?

What the Commission should be exploring

- The structure and impact of clear, sector-specific industry standards can promote safety of AI systems.
- The role of regulation or suggestive guidance in the trading marketplace versus voluntary commitments.
- The impact of a civil rights-based review for any AI system that could affect individuals’ legal rights.
- The positioning of consumer and industry disclosures.

THANK YOU!

Nicol Turner Lee, Senior Fellow and Director of the Center for Technology Innovation, Brookings Institution

nturnerlee@brookings.edu

@drturnerlee (Twitter) and Nicol Lee (LinkedIn)

Impact Assessment of AI on Cybersecurity Threats

Dan Guido, *Co-founder & CEO, Trail of Bits*

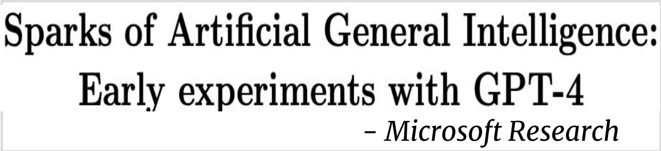
CFTC Technology Advisory Committee (TAC) Meeting
July 18, 2023

AI capabilities are rising rapidly, or are they?

+

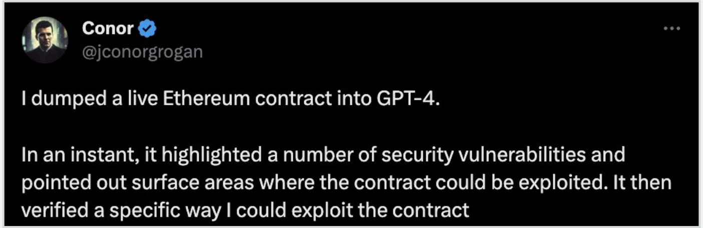
Proponents

AI is effectively magic and ready to take over for general intelligence.



Sparks of Artificial General Intelligence: Early experiments with GPT-4

– Microsoft Research



Conor @jconorgrogan

I dumped a live Ethereum contract into GPT-4.

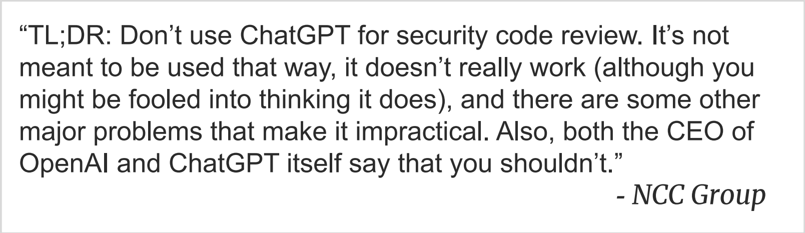
In an instant, it highlighted a number of security vulnerabilities and pointed out surface areas where the contract could be exploited. It then verified a specific way I could exploit the contract

−

Opponents

AI is useless and parrot out nonsense from their training data.

GPT-4 Might Just Be a Bloated, Pointless Mess *– The Atlantic*



"TL;DR: Don't use ChatGPT for security code review. It's not meant to be used that way, it doesn't really work (although you might be fooled into thinking it does), and there are some other major problems that make it impractical. Also, both the CEO of OpenAI and ChatGPT itself say that you shouldn't."

- NCC Group

… sometimes these are the same people:

"GPT-4 performed poorly at building exploits for the vulnerabilities" *- OpenAI*

Empirical results from Trail of Bits

What we realized:

- AI is just another tool, not magic
- Ask the right questions
- Evaluate progress correctly
- Choose the right problem

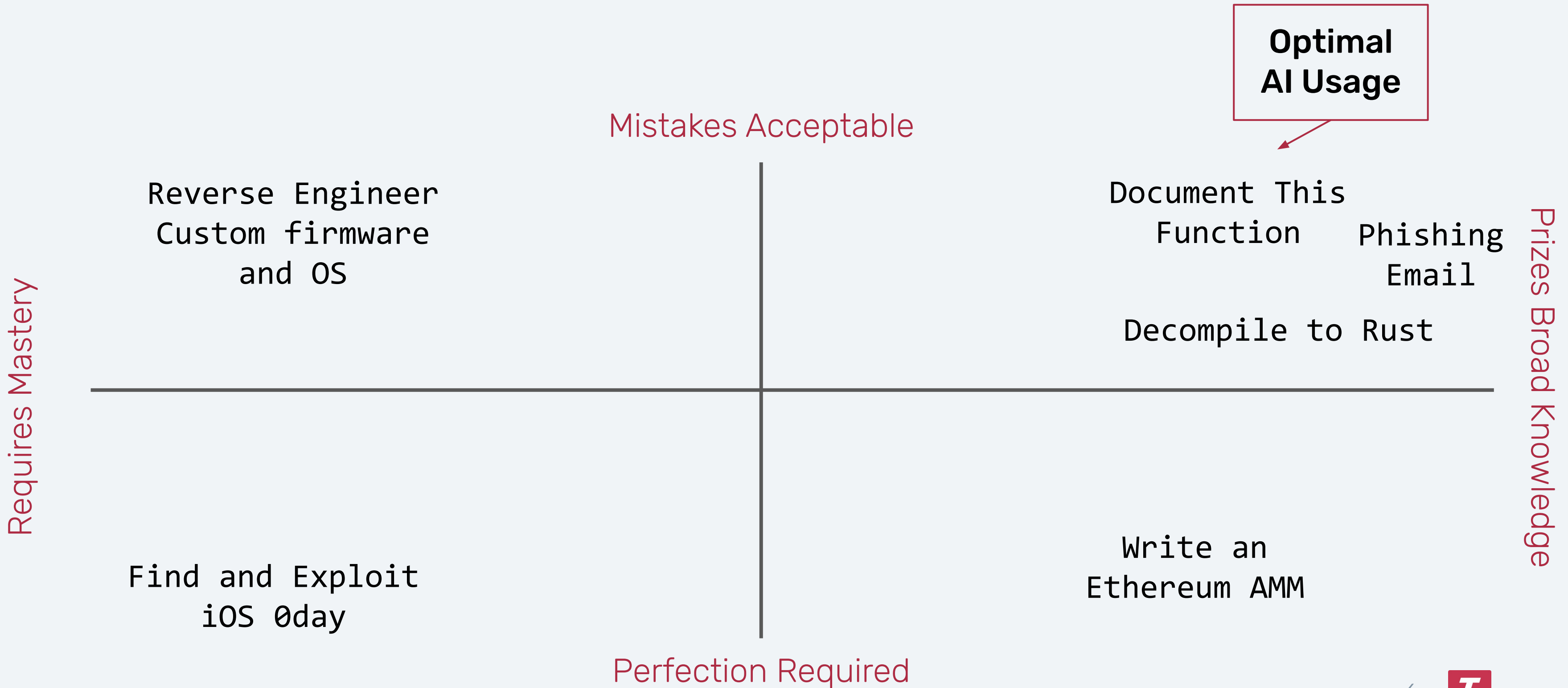
Don’t obsess about complete automation. What constraints are blocking humans from being more productive?

Our successes with AI:

- Decompile code into high-level languages
- Identify and trigger bugs
- Reason about memory layouts
- Write scripts to launch exploits
- Identify weak static encryption
- Find cryptographic API misuse

It won't write an exploit for you, but it can make exploit writing more productive.

What can AI [currently] do?



Optimal AI Usage

Mistakes Acceptable

Perfection Required

Requires Mastery

Prizes Broad Knowledge

Reverse Engineer Custom firmware and OS

Document This Function

Phishing Email

Decompile to Rust

Find and Exploit iOS 0day

Write an Ethereum AMM

Fields that are disrupted first

Bug bounties

- Incentives align perfectly to spam bounty submissions with AI
- ChatGPT's reports sound plausible and are written well
- Only a highly paid expert can unravel the mystery.

Phishing training

You can create native-speaker level human language at speed and scale now

- ChatGPT may already know about you. It knows me!
- "Write a perfect phishing message for Dan Guido."

Signature-Based Defenses

Changing signatures is a language translation problem. AI is very good at language translation problems. E.g., IDS, AV.

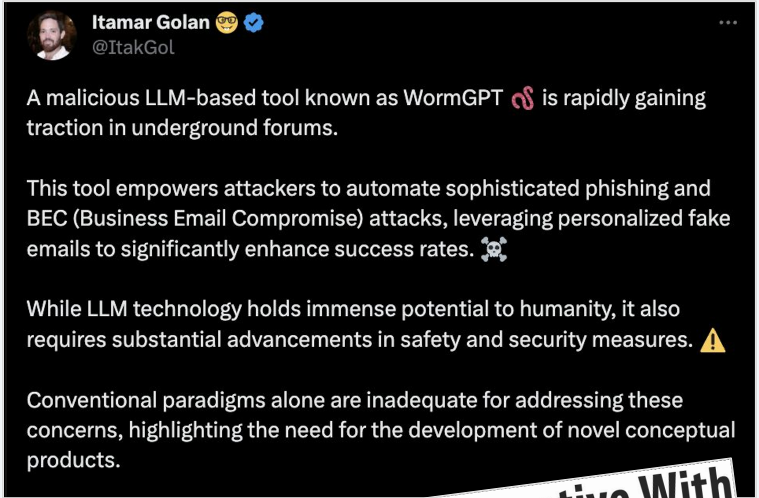
Attacker Attribution

Attribution is style detection; AI is very good at style transfer.

It's asymmetric warfare,
and incentives align against these specific defenses

Alignment will not save you

- **RLHF-based alignment doesn't work**
  - Output censorship is an unwinnable task that mainly frustrates amateurs and researchers
  - AI can't unlearn it was trained on hacking techniques
  - Example: "DAN" aka "Do Anything Now"
- **Open-source models are available**
  - Not bound by US regulations. Current best open source model (Falcon-40B) is from the UAE.
  - They are becoming quite good
  - Criminals are already using them



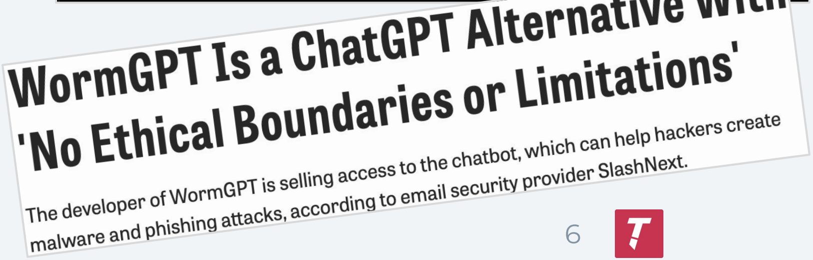
Itamar Golan 🤓 ✓
@ItakGol

A malicious LLM-based tool known as WormGPT 🪱 is rapidly gaining traction in underground forums.

This tool empowers attackers to automate sophisticated phishing and BEC (Business Email Compromise) attacks, leveraging personalized fake emails to significantly enhance success rates. ☠️

While LLM technology holds immense potential to humanity, it also requires substantial advancements in safety and security measures. ⚠️

Conventional paradigms alone are inadequate for addressing these concerns, highlighting the need for the development of novel conceptual products.

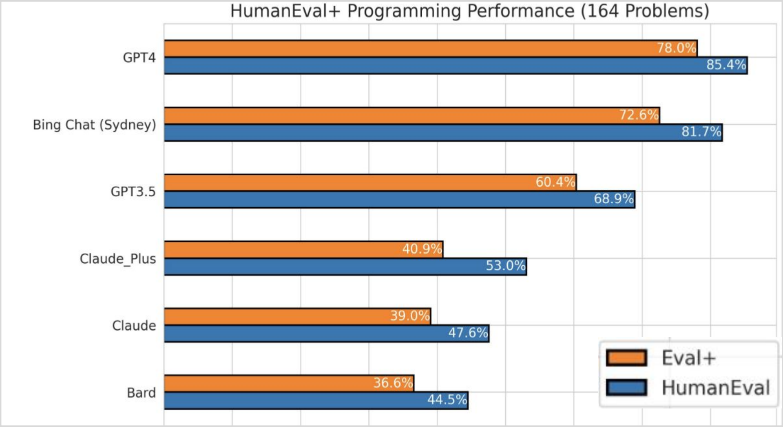


WormGPT Is a ChatGPT Alternative With 'No Ethical Boundaries or Limitations'

The developer of WormGPT is selling access to the chatbot, which can help hackers create malware and phishing attacks, according to email security provider SlashNext.

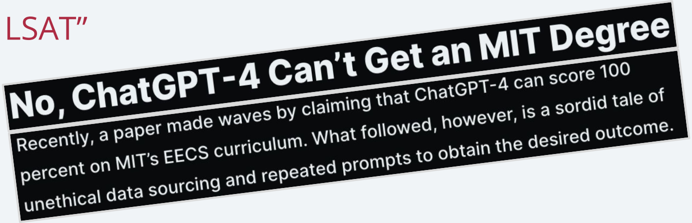
Their limits are unknown without measurements

- **ML evaluations have focused on programming, not cybersecurity**
  - No effective systematic evaluations for emergent cyber capabilities
- **Needed: taxonomies and benchmarks for offensive capabilities**
  - Model capabilities versus those of state-of-the-art security tools
  - Compare capabilities of human operators with varying expertise using LLMs
  - Classify opportunities/risks of downstream impacts



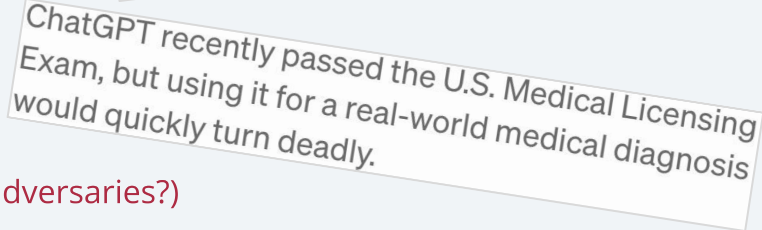
When does AI fundamentally change industry risk?

1. **Looking past hype and advertising**
   - Is the problem in the training set? Think “GPT4 passes the LSAT”
   - Does the output generalize past one or few examples?
   - What happens when the AI is wrong? It will be wrong.
2. **We need more measurement**
   - Task specific data sets and evaluation frameworks
3. **Identifying risk-changing capability**
   - Does this remove a hard constraint for me (or my adversaries?)
   - How rapidly is the capability likely to improve?
   - Is there a synergy with existing, unrelated technologies?
   - Are mistakes acceptable, or easy to catch?



No, ChatGPT-4 Can’t Get an MIT Degree

Recently, a paper made waves by claiming that ChatGPT-4 can score 100 percent on MIT’s EECS curriculum. What followed, however, is a sordid tale of unethical data sourcing and repeated prompts to obtain the desired outcome.



ChatGPT recently passed the U.S. Medical Licensing Exam, but using it for a real-world medical diagnosis would quickly turn deadly.

AI is a systemic threat to cybersecurity

Key takeaways

- AI changes the cost model for attackers and defenders
- AI will augment human capability, not replace it
- Alignment is a distraction: potential harms are here today
- Measurement is needed to eliminate surprise

Short-term predictions

- Algorithmic tools are not disappearing
- More local and open source models and infrastructure
- Prepare for disruption today, because it's coming
- With investment, defense may benefit more from AI

Resources

Can AI beat humans in security audits?

Curated references for ML security

What effect will AI have on national security?

How to measure safety of AI-based systems

CFTC

COMMODITY FUTURES TRADING COMMISSION

Topic 2: Regulatory Issues for DeFi, Including DAOs

CFTC

COMMODITY FUTURES TRADING COMMISSION

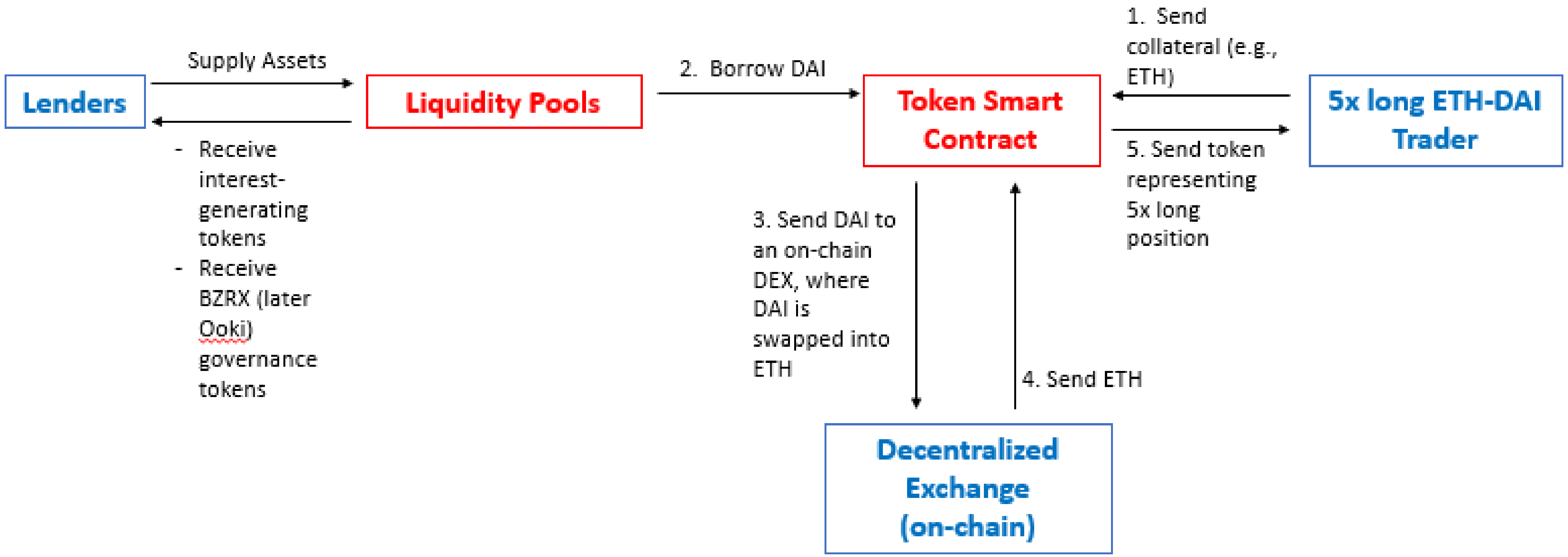
Enforcement Case Study: Ooki DAO

Anthony Biagioli, Special Counsel to the Director,
Division of Enforcement, CFTC

July 18, 2023

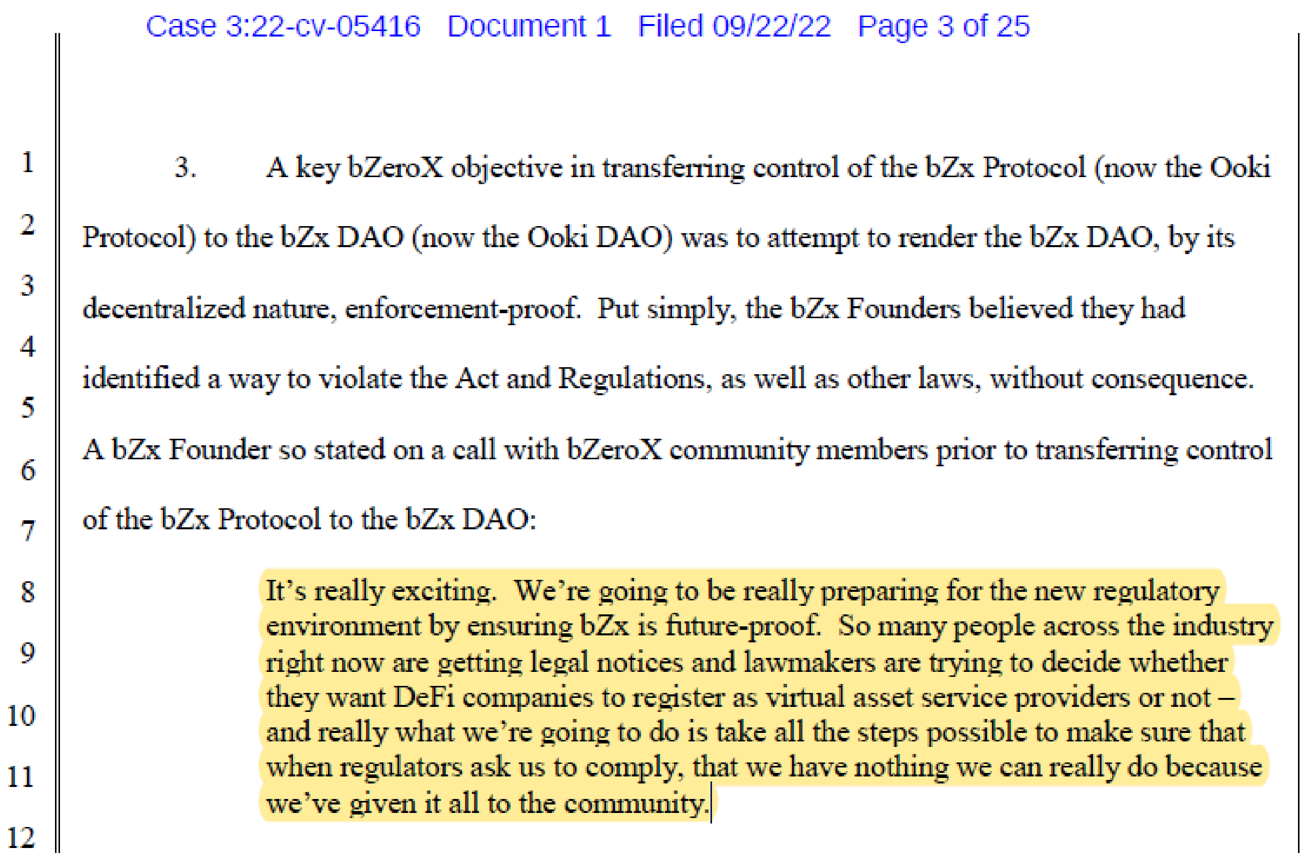
Enforcement Case Study: Ooki DAO

- Mechanics of opening leveraged position on bZx Protocol (later Ooki Protocol) (simplified sample):


Lenders
Supply Assets
Liquidity Pools
- Receive interest-generating tokens
- Receive BZRX (later Ooki) governance tokens
2. Borrow DAI
Token Smart Contract
1. Send collateral (e.g., ETH)
5x long ETH-DAI Trader
5. Send token representing 5x long position
3. Send DAI to an on-chain DEX, where DAI is swapped into ETH
4. Send ETH
Decentralized Exchange (on-chain)

Enforcement Case Study: Ooki DAO

- Statement of bZeroX, LLC founder to DAO community upon creating the DAO.



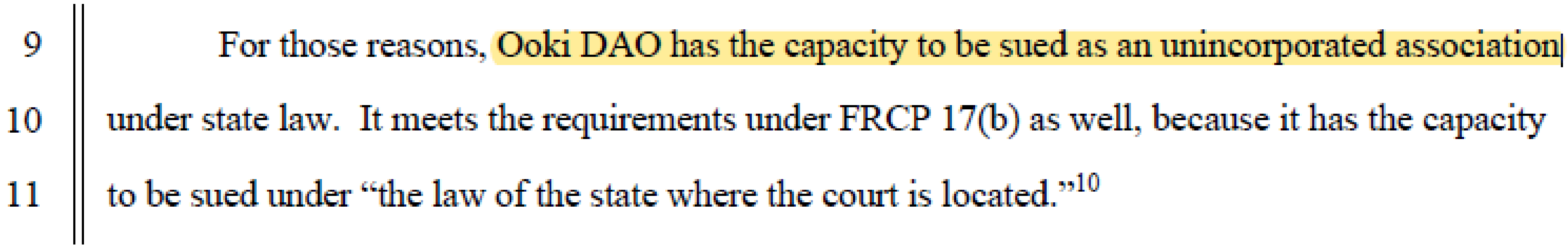
Case 3:22-cv-05416 Document 1 Filed 09/22/22 Page 3 of 25

3. A key bZeroX objective in transferring control of the bZx Protocol (now the Ooki Protocol) to the bZx DAO (now the Ooki DAO) was to attempt to render the bZx DAO, by its decentralized nature, enforcement-proof. Put simply, the bZx Founders believed they had identified a way to violate the Act and Regulations, as well as other laws, without consequence. A bZx Founder so stated on a call with bZeroX community members prior to transferring control of the bZx Protocol to the bZx DAO:

> It's really exciting. We're going to be really preparing for the new regulatory environment by ensuring bZx is future-proof. So many people across the industry right now are getting legal notices and lawmakers are trying to decide whether they want DeFi companies to register as virtual asset service providers or not – and really what we're going to do is take all the steps possible to make sure that when regulators ask us to comply, that we have nothing we can really do because we've given it all to the community.

Enforcement Case Study: Ooki DAO

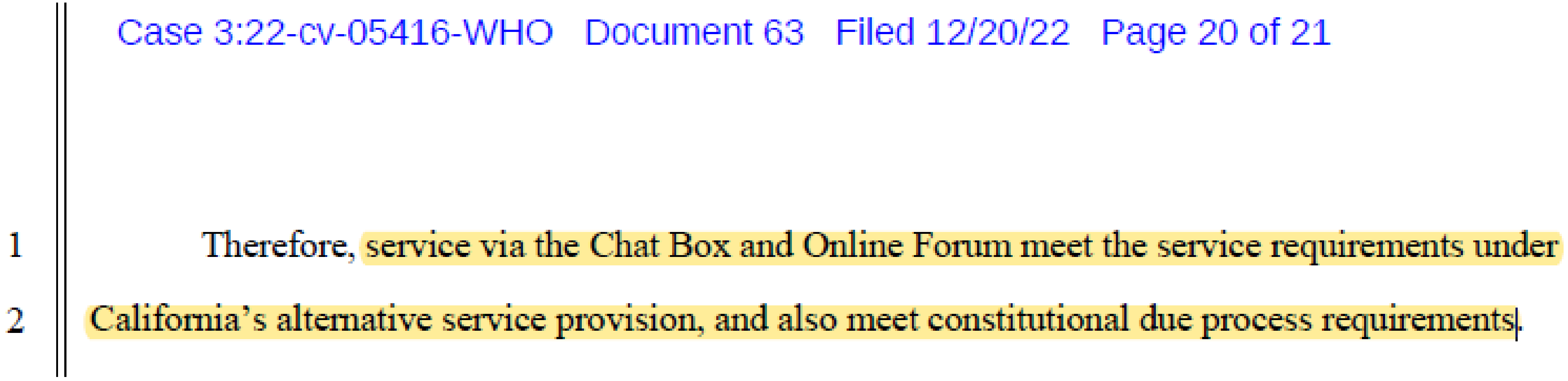
- N.D. Cal. holds: Ooki DAO can be sued as unincorporated association.



For those reasons, Ooki DAO has the capacity to be sued as an unincorporated association under state law. It meets the requirements under FRCP 17(b) as well, because it has the capacity to be sued under “the law of the state where the court is located.”[10]

Enforcement Case Study: Ooki DAO

- N.D. Cal. holds: Ooki DAO can be served as unincorporated association.

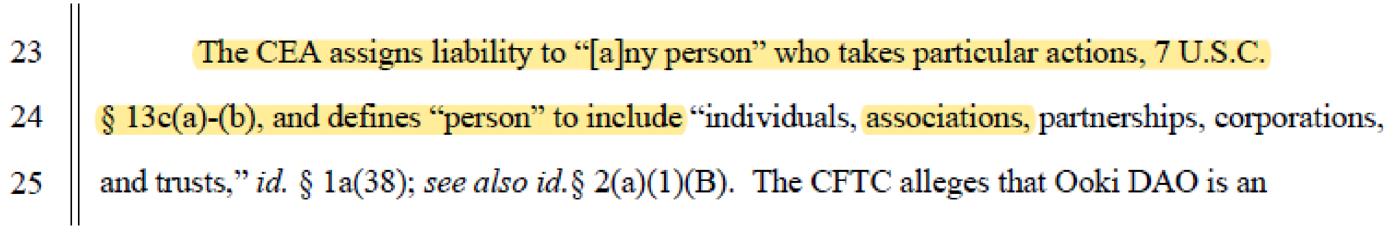


Case 3:22-cv-05416-WHO Document 63 Filed 12/20/22 Page 20 of 21

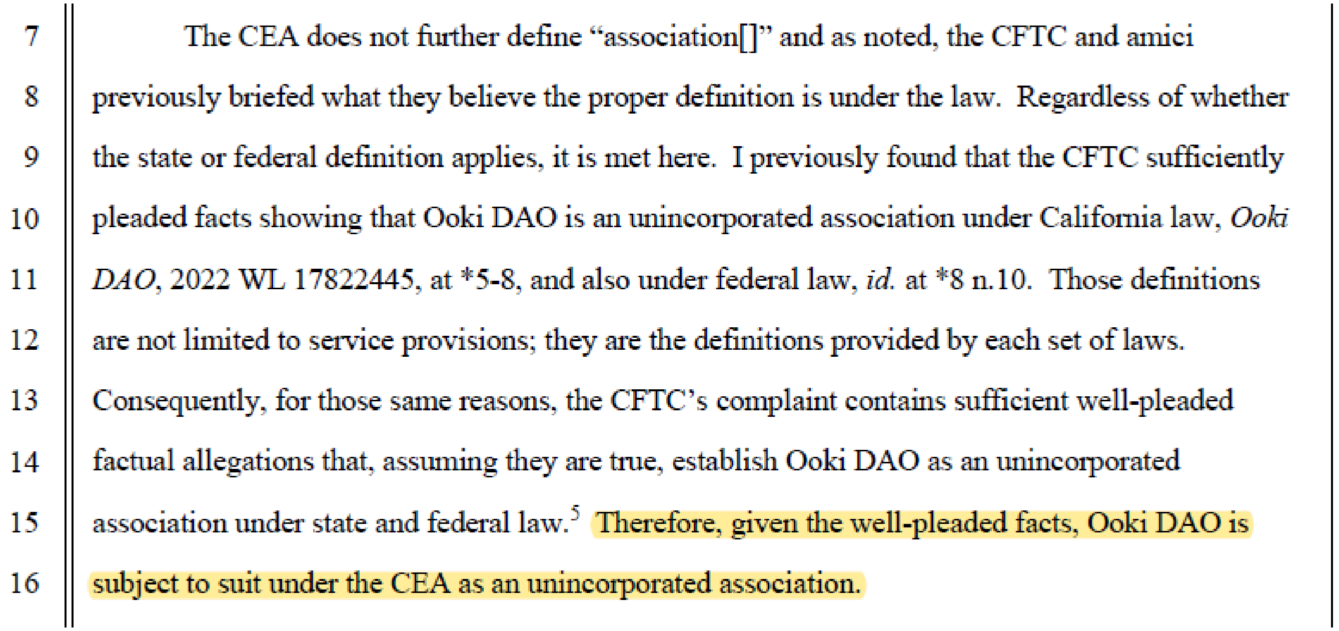
Therefore, service via the Chat Box and Online Forum meet the service requirements under California’s alternative service provision, and also meet constitutional due process requirements.

Enforcement Case Study: Ooki DAO

- N.D. Cal. holds: Ooki DAO is a “person” under the CEA.



The CEA assigns liability to “[a]ny person” who takes particular actions, 7 U.S.C. § 13c(a)-(b), and defines “person” to include “individuals, associations, partnerships, corporations, and trusts,” *id.* § 1a(38); *see also id.*§ 2(a)(1)(B). The CFTC alleges that Ooki DAO is an



The CEA does not further define “association[]” and as noted, the CFTC and amici previously briefed what they believe the proper definition is under the law. Regardless of whether the state or federal definition applies, it is met here. I previously found that the CFTC sufficiently pleaded facts showing that Ooki DAO is an unincorporated association under California law, *Ooki DAO*, 2022 WL 17822445, at *5-8, and also under federal law, *id.* at *8 n.10. Those definitions are not limited to service provisions; they are the definitions provided by each set of laws. Consequently, for those same reasons, the CFTC’s complaint contains sufficient well-pleaded factual allegations that, assuming they are true, establish Ooki DAO as an unincorporated association under state and federal law.[5] Therefore, given the well-pleaded facts, Ooki DAO is subject to suit under the CEA as an unincorporated association.

DISCLAIMER

The analyses and views expressed herein are those of the authors and do not necessarily reflect the views of the Commission or CFTC Staff.

Shifting focus to smart contracts

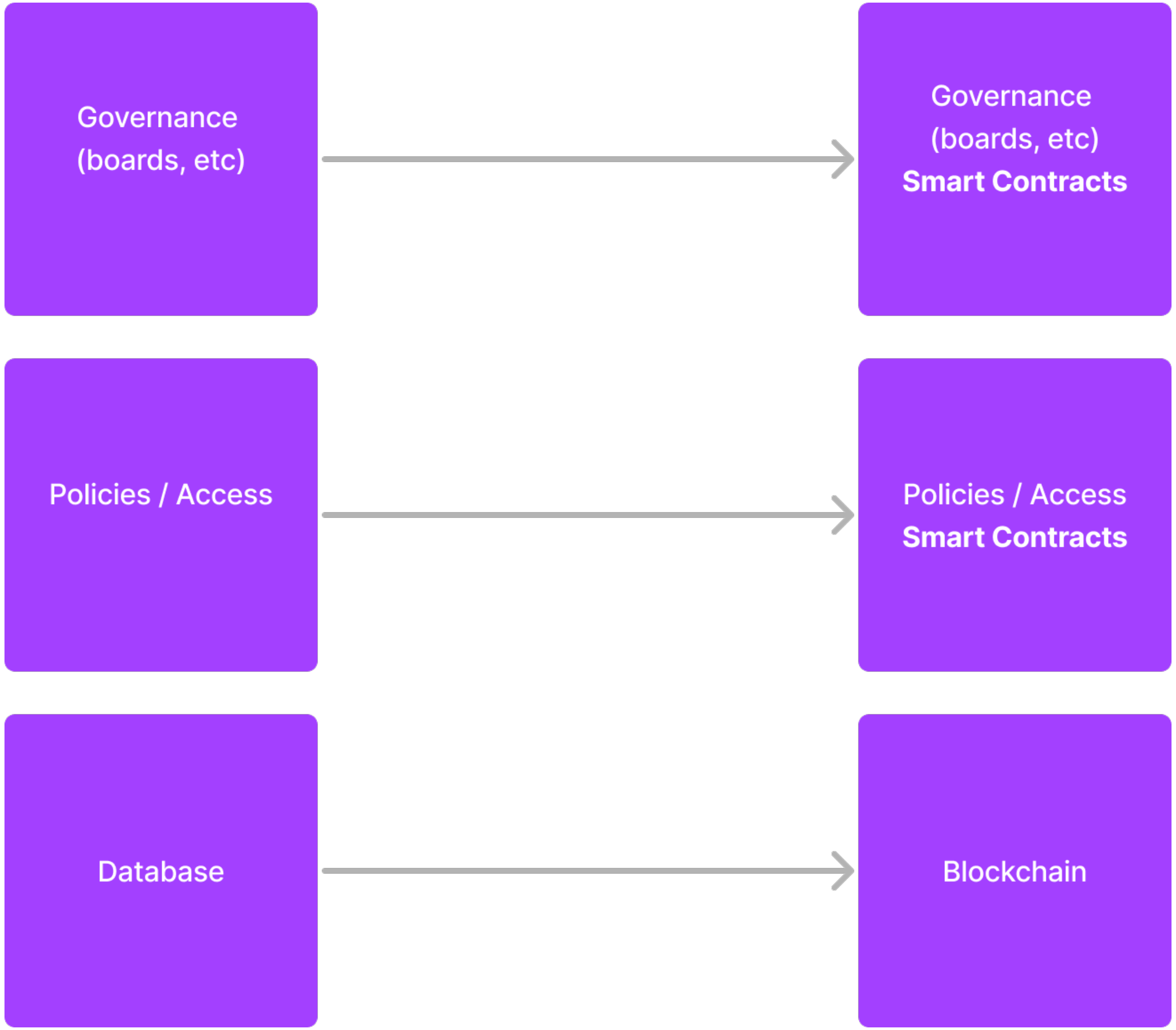
“the term (DAO) is only understood today as organizations deployed as smart contracts on top of an existing blockchain network” ~ Wikipedia

In a traditional system: These systems are reflected in articles, complemented by internal policies, and overseen by committees, boards, and other standard governance methods.

Traditional

Smart Contract based system

Parallels



Governance (boards, etc)

Governance (boards, etc)
Smart Contracts

Policies / Access

Policies / Access
Smart Contracts

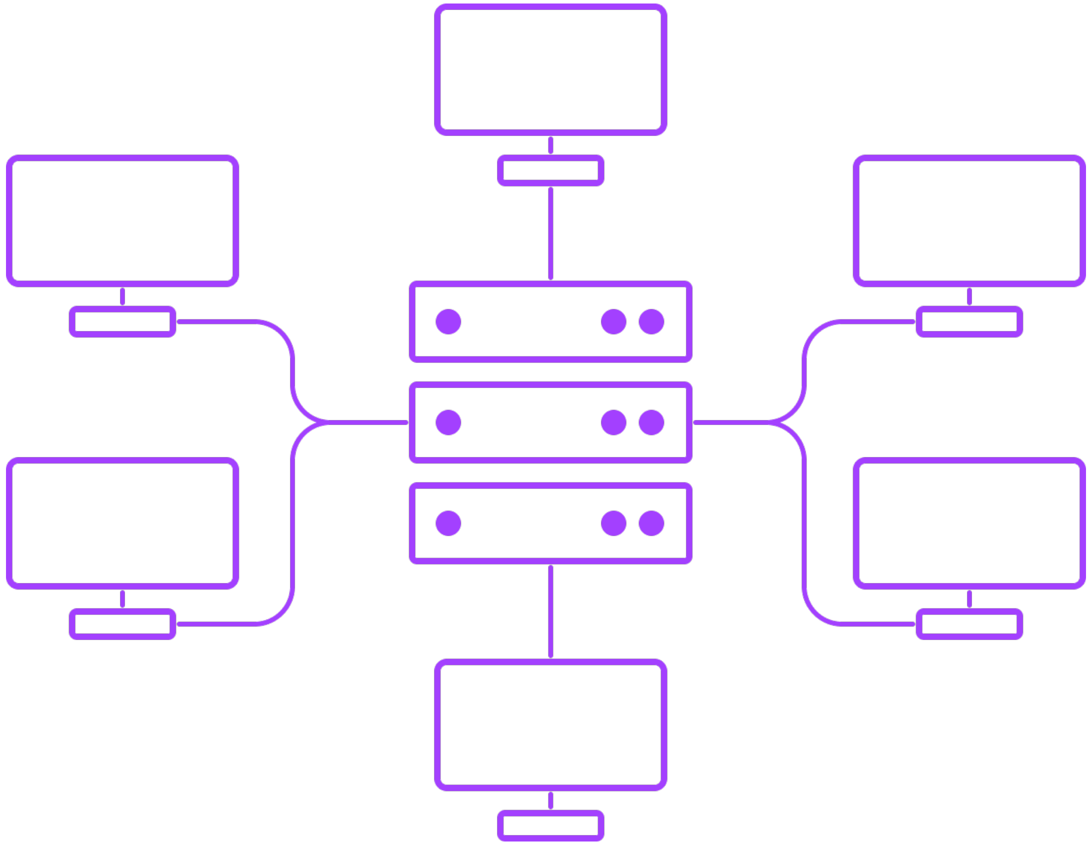
Database

Blockchain

Key differences moving from traditional to smart contracts

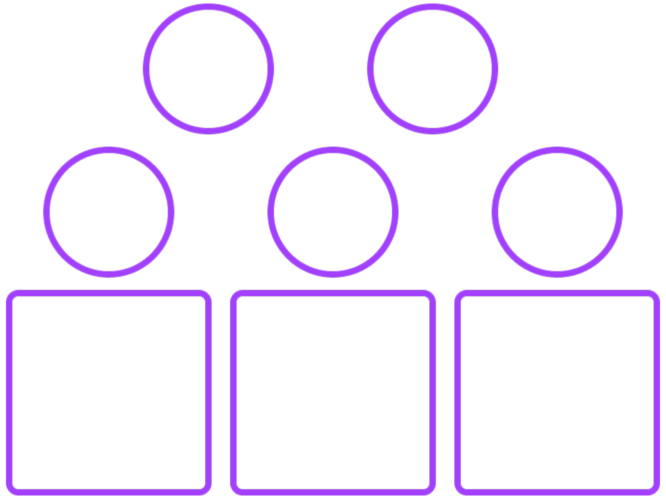
Meeting / vote

Signing ceremony

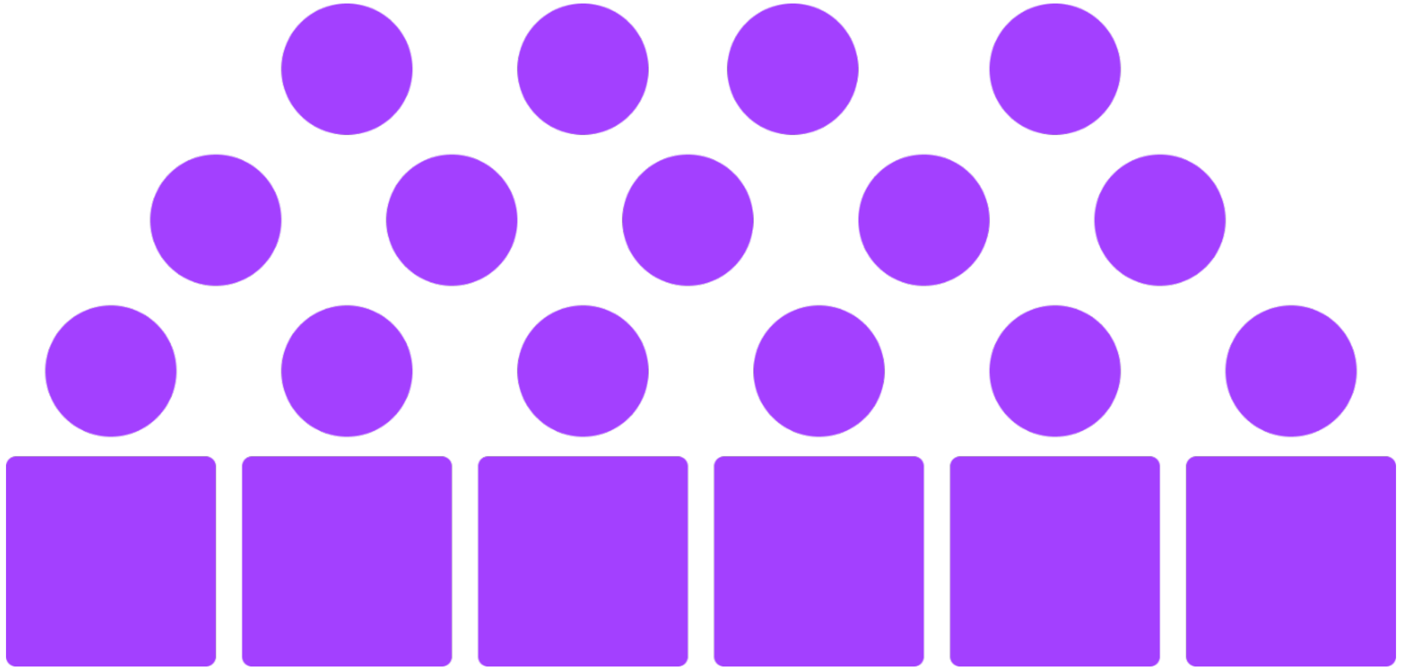


Outcomes of voting

Vote is private by default



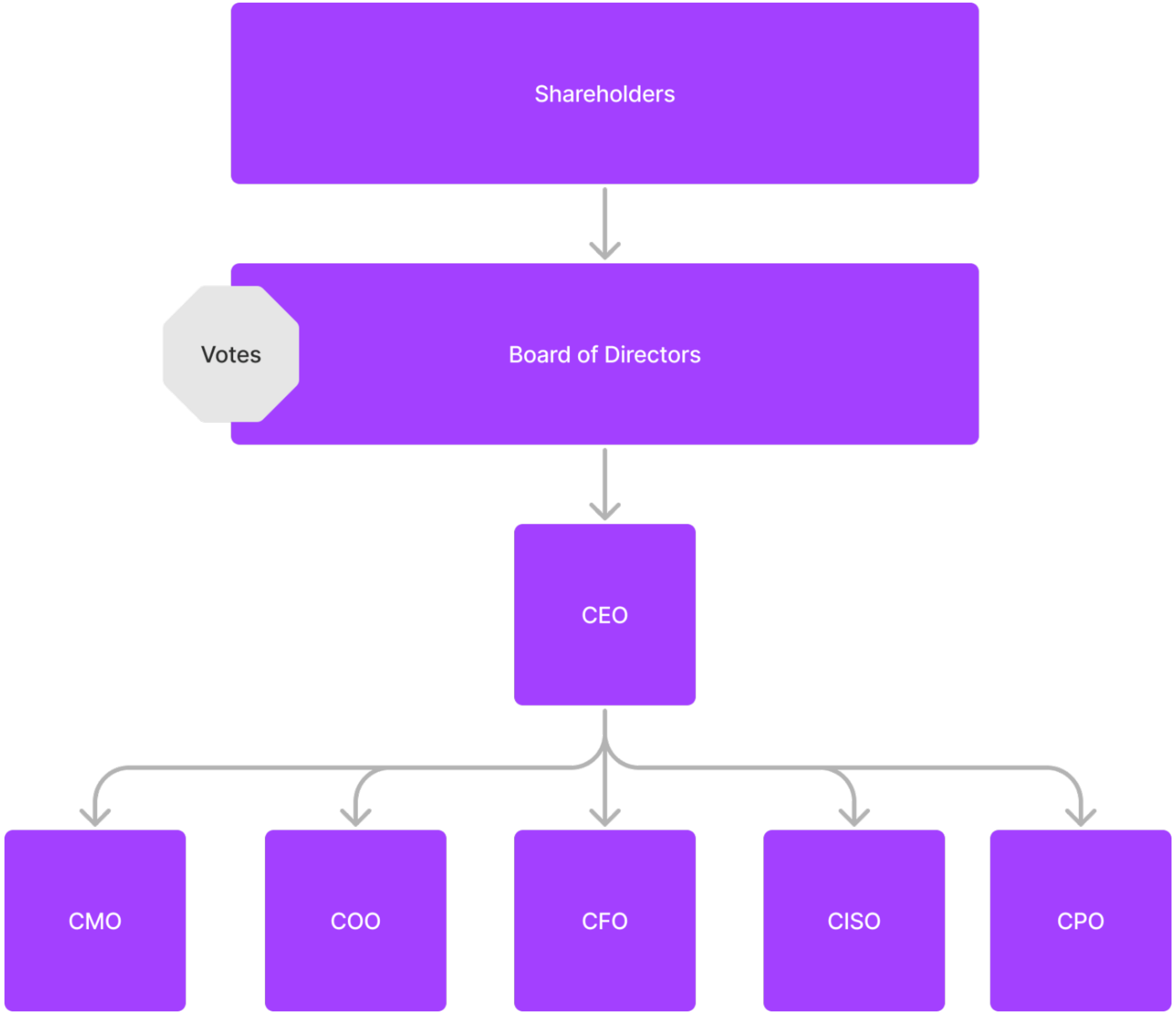
Vote is public by default



Smart contracts can engage in regulated functions, but not all do

If a smart contract engages in a regulated function on behalf of someone, it is the same as any other computer code executing a similar function.

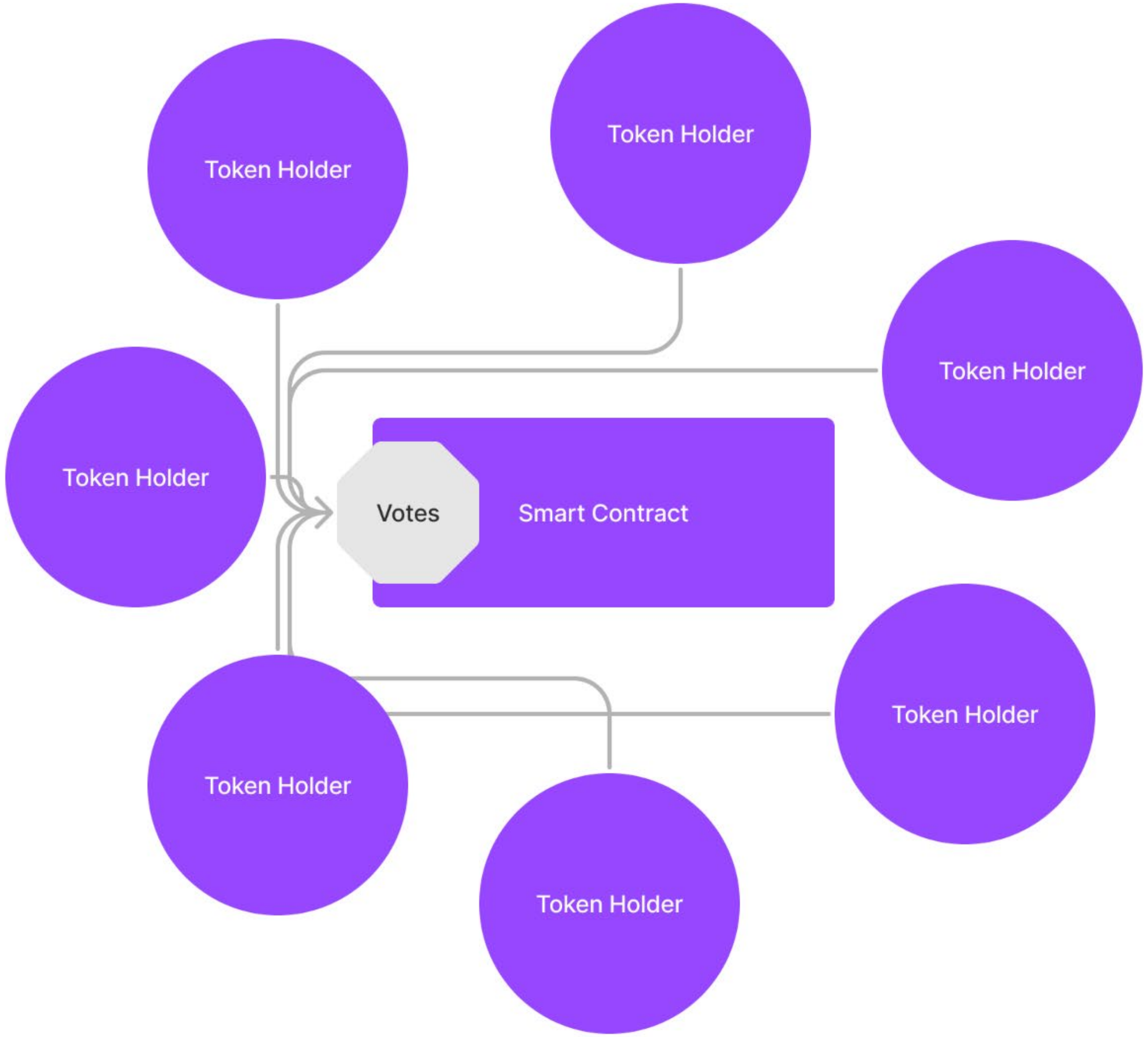
Smart contracts can also be used as a regulated entities basic voting and recording mechanisms or to create products.


Shareholders
Votes
Board of Directors
CEO
CMO
COO
CFO
CISO
CPO

Using smart contracts as a governance model

Token holders can vote as a traditional board would vote on an initiative.

Smart contracts can subsequently reference other smart contracts to automate various behaviors.



```
contract BonusDAO {
    // Structure to represent a payment proposal
    struct PaymentProposal {
        address payable recipient;  // Address to receive the payment
        uint256 amount;             // Amount to be paid
        uint256 yesVotes;           // Total "yes" votes
        uint256 noVotes;            // Total "no" votes
        bool released;              // Flag indicating if the payment has been released
        mapping(address => bool) voted;  // Mapping to keep track of voters
    }

    address public admin;                   // Address of the contract administrator
    mapping(uint256 => PaymentProposal) public proposals;  // Mapping of proposal IDs to PaymentProposal objects
    uint256 public proposalCount;           // Total number of payment proposals

    // Events to be emitted
    event ProposalCreated(uint256 indexed proposalId, address indexed recipient, uint256 amount);
    event Voted(uint256 indexed proposalId, address indexed voter, bool indexed inSupport);
    event PaymentReleased(uint256 indexed proposalId, address indexed recipient, uint256 amount);

    // Modifier to restrict access to the contract administrator
    modifier onlyAdmin() {
        require(msg.sender == admin, "Only the contract administrator can perform this action");
        _;
    }

    // Modifier to check if a proposal exists
    modifier validProposal(uint256 proposalId) {
        require(proposalId > 0 && proposalId <= proposalCount, "Invalid proposal ID");
        _;
    }

    constructor() {
        admin = msg.sender;  // Set the contract creator as the administrator
    }

    // Function to create a payment proposal
    function createProposal(address payable _recipient, uint256 _amount) external onlyAdmin {
        proposalCount++;
        proposals[proposalCount] = PaymentProposal(_recipient, _amount, 0, 0, false);
        emit ProposalCreated(proposalCount, _recipient, _amount);
    }
```

```
0x2d78d40DcFb4C0299B312EaF0374c7Df591FDd64
0x7dA7B2eFc4Bdd071Cb8c2c0d6B4Df4893f9EF482
0xA6aD84Dc84Cb63F405E6857bDa208C91Ea6531E5
0xFf75171B2a4b7c35C1cC29C10d61C75d80a4BdB1
0x4c7D15Cd5e4a6D2e7c692e6D64873A246Cdb1b17
0xd768f3cD63d9804f2b1fDe4C8d9D4EfACab0dEf6
0x9f8d6E8265EF60AcF4Ad546a723603a3A3710E5A
0xB77B0D99f1799c22A8e2e4d972B79AC8E1a9F96f
0xC90a33aC6aC4b193dEECE66D37D2DD045eC6029F
0x1458d8EaaDd3Bf7F70a1544E7b4De734De5cC2e5
0x826cC1C06eDD0079CFeD18F63dF71B3e1B535d04
0xF4f2c6A1f3dD06625eB3D066B079f5f3fCf5Ae94
```

```
contract BonusDAO {
    // Structure to represent a payment proposal
    struct PaymentProposal {
        address payable recipient;  // Address to receive the payment
        uint256 amount;             // Amount to be paid
        uint256 yesVotes;           // Total "yes" votes
        uint256 noVotes;            // Total "no" votes
        bool released;              // Flag indicating if the payment has been released
        mapping(address => bool) voted;  // Mapping to keep track of voters
    }

    address public admin;                  // Address of the contract administrator
    mapping(uint256 => PaymentProposal) public proposals;  // Mapping of proposal IDs to PaymentProposal objects
    uint256 public proposalCount;           // Total number of payment proposals

    // Events to be emitted
    event ProposalCreated(uint256 indexed proposalId, address indexed recipient, uint256 amount);
    event Voted(uint256 indexed proposalId, address indexed voter, bool indexed inSupport);
    event PaymentReleased(uint256 indexed proposalId, address indexed recipient, uint256 amount);

    // Modifier to restrict access to the contract administrator
    modifier onlyAdmin() {
        require(msg.sender == admin, "Only the contract administrator can perform this action");
        _;
    }

    // Modifier to check if a proposal exists
    modifier validProposal(uint256 proposalId) {
        require(proposalId > 0 && proposalId <= proposalCount, "Invalid proposal ID");
        _;
    }

    constructor() {
        admin = msg.sender;  // Set the contract creator as the administrator
    }

    // Function to create a payment proposal
    function createProposal(address payable _recipient, uint256 _amount) external onlyAdmin {
        proposalCount++;
        proposals[proposalCount] = PaymentProposal(_recipient, _amount, 0, 0, false);
        emit ProposalCreated(proposalCount, _recipient, _amount);
    }
```

```
contract TradeExecutor {
    address public contractToWatch;  // Address of the contract to
monitor
    address public tradeCounterparty;  // Address of the trade
counterparty
    uint256 public tradeAmount;  // Amount to trade

    constructor(address _contractToWatch, address
_tradeCounterparty, uint256 _tradeAmount) {
        contractToWatch = _contractToWatch;
        tradeCounterparty = _tradeCounterparty;
        tradeAmount = _tradeAmount;
    }

    function executeTrade() external {
        // Assume some behavior is being monitored in the
contractToWatch
        // When the desired behavior is observed, execute the trade
        // Here, we assume the desired behavior is calling a specific
function
        // Check if the desired function has been called in the
contractToWatch
        bool desiredBehavior =
ContractToWatch(contractToWatch).hasCalledFunction();

        if (desiredBehavior) {
            // Perform the trade with the tradeCounterparty
            // ... perform the trade logic here ...
            // For the sake of example, let's assume it transfers Ether to the
tradeCounterparty
            payable(tradeCounterparty).transfer(tradeAmount);
        }
    }
}

contract ContractToWatch {
    // Assume some behavior being monitored
    function hasCalledFunction() external pure returns (bool) {
        // ... implementation of the desired behavior ...
        // For the sake of example, let's assume it returns true
        return true;
    }
}
```

```
0x2d78d40DcFb4C0299B312EaF0374c7Df591FDd64
0x7dA7B2eFc4Bdd071Cb8c2c0d6B4Df4893f9EF482
0xA6aD84Dc84Cb63F405E6857bDa208C91Ea6531E5
0xFf75171B2a4b7c35C1cC29C10d61C75d80a4BdB1
0x4c7D15Cd5e4a6D2e7c692e6D64873A246Cdb1b17
0xd768f3cD63d9804f2b1fDe4C8d9D4EfACab0dEf6
0x9f8d6E8265EF60AcF4Ad546a723603a3A3710E5A
0xB77B0D99f1799c22A8e2e4d972B79AC8E1a9F96f
0xC90a33aC6aC4b193dEECE66D37D2DD045eC6029F
0x1458d8EaaDd3Bf7F70a1544E7b4De734De5cC2e5
0x826cC1C06eDD0079CFeD18F63dF71B3e1B535d04
0xF4f2c6A1f3dD06625eB3D066B079f5f3fCf5Ae94
```

Considerations

1. Speed / Cost
   a. Blockchain
2. Privacy / Security
   a. Blockchain
3. Regulatory Mapping
   a. Blockchain-agnostic

Speed/Cost

Ethereum Wire Transfer	$5	ETH: Ranges $1 - $10 Wire: $5 Bank / $20 Business
Avalanche ACH	$0.05	
Stellar Database Transfer	$0.000001	

Balancing centralization vs. decentralization (privacy/security)

- Hypothetically, the smart contract is deployed on a decentralized protocol. It could be deployed on a private centralized blockchain.

- What is still centralized? Who can vote? Who can update the contract? Who holds the keys? Where the people are, where the customers are, what the products are. The blockchain could also be centralized.. Confused yet?

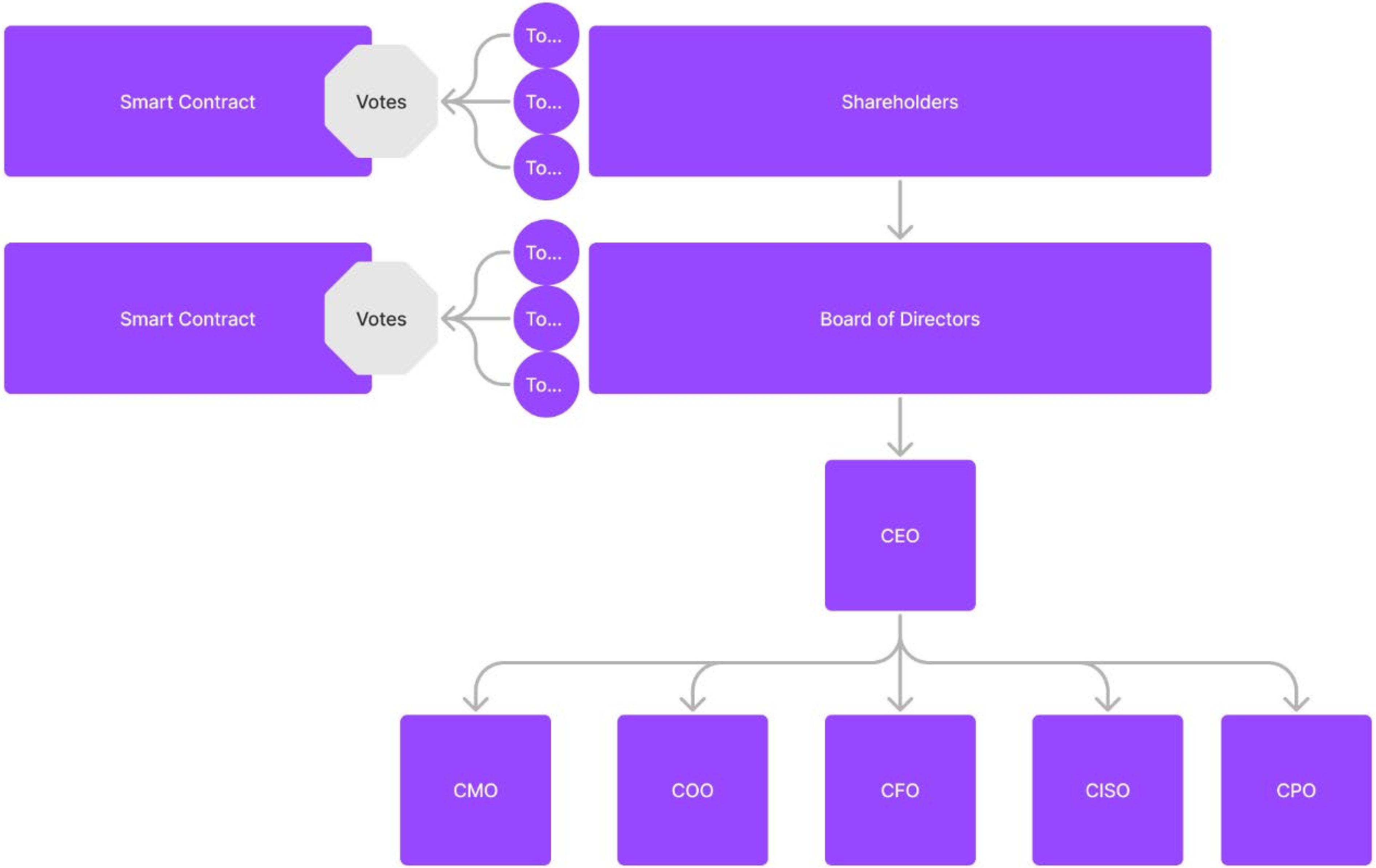
Permissed/Private based blockchains are now viable

	Avalanche Subnets	Polygon Edge/Supernets	Cosmos SDK
Projects Launched	23	35	54
Consensus	Snowman Consensus Protocol	IBFT PoS, Configurable IBFT PoA	Tendermint
Customizable VM	Yes	No	Yes
TPS	4500+	1500+	Thousands
Finality	< 2 seconds (probabilistic)	Instant ~ 2 seconds block (deterministic)	Instant ~ 1 second block
Validator Staking Requirements	2,000 AVAX ~ 34,000 USDC	20,000 MATIC 13,400 USDC*	Variable

Hypothetical use of smart contracts in current regulatory structure

Many participants, all could be known to one another. All are known to the regulator.

Different participants might have different powers or use different blockchains or a hybrid database approach. Some votes or acknowledgements may be required to be private.



Smart Contract

Votes

To...

To...

To...

Shareholders

Smart Contract

Votes

To...

To...

To...

Board of Directors

CEO

CMO

COO

CFO

CISO

CPO

Elvis Presley

0xd8dA6BF26964aF9D7eEd9e03E
53415D37aA96045

LEDGER

WESPER

Immediate applications

Use smart contracts when they solve a problem and focus on mapping them to the existing regulation. This should work wonderfully & provide an audit trail of decisions made.

Technology & people regulation

When smart contracts are operated by people, regulation is applied to the jurisdictions where the operators are, where the end user is, and the functions of the project. Same as technology built on traditional databases.

Starting at first principles and understanding the technology, we can understand how much of our current regulation applies to the new technology. Only then, can we really appreciate what new regulation is needed to create additional coverage.

Open questions

Who should be treated as the responsible operator of a smart contract engaging in a regulated function? Voter / key holder / benefactor / contract deployer?

How does regulation apply when a person is not involved in the creation of the code, it is entirely decentralized, and there is no personal benefit?

IPFS

Pinata

CLOUDFLARE

Decentralization, DeFi & Governance

What DeFi is, what it can be, and what it means for regulation

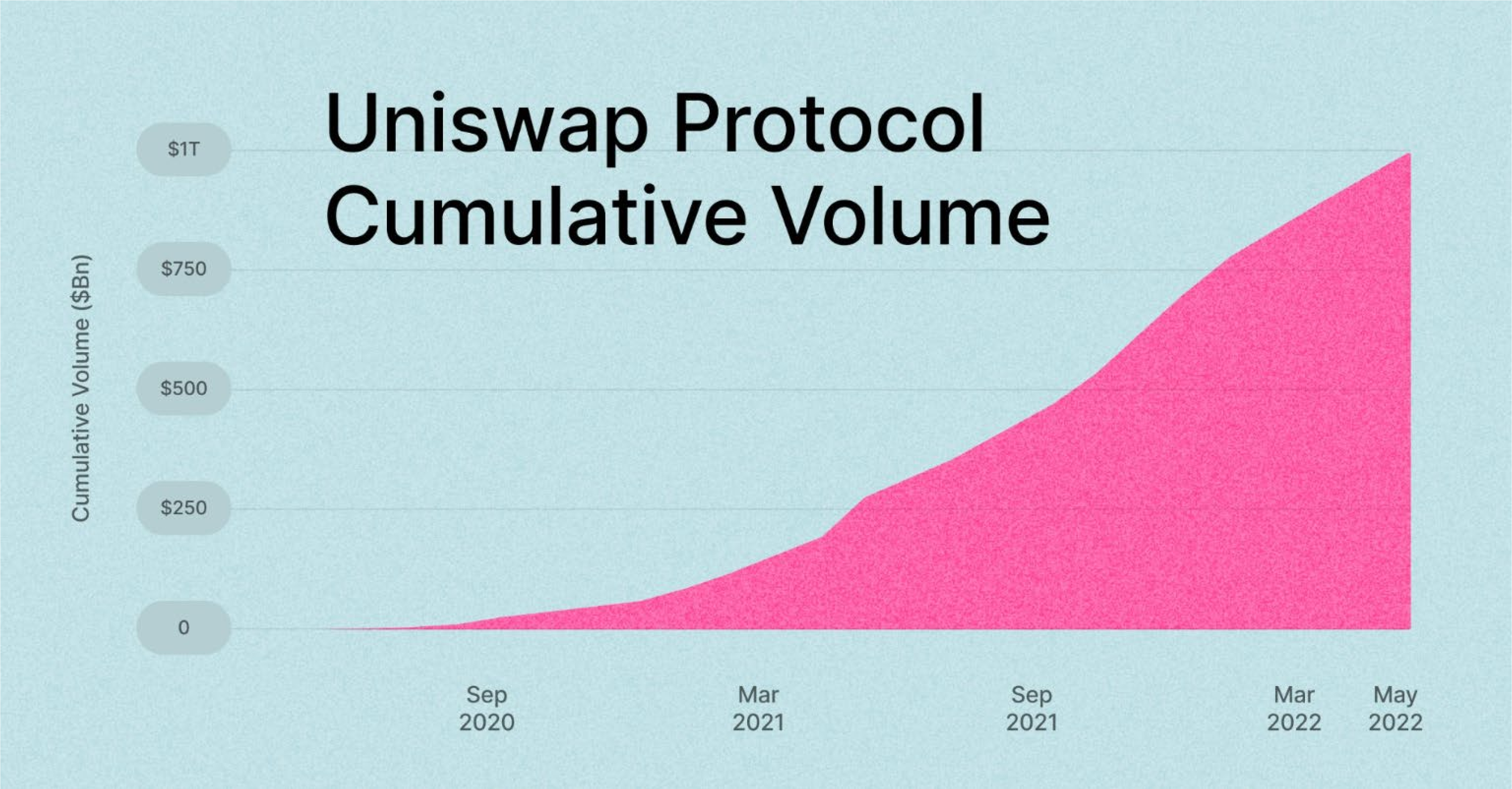
Context

- Defi remains a relatively recent innovation, even for crypto

- Four key concepts
    - Self custody
    - Autonomous
    - Transparent
    - Interoperable and Composable

- Decentralization is a spectrum, not a toggle

DeFi in the Wild



DeFi Governance

- Natural tension between heavy governance and DeFi
    - Our view is the core virtue of DeFi is credible neutrality
        - Dependability
        - Avoiding capture
    - By definition, the greater the governance, the greater the risk of capture

- The true value of DeFi is found when the governance itself could be said to shrink down to the point of imperceptibly

What DeFi Governance is Not

- Something that can ever fully go away
  - Essential governance

- Constant formality
  - Stakeholders groups are protean

The Optimal Approach: Governance Minimization

- Flexibility
  - Game theory-driven systems

- Distinguish between tokenholders and stakeholders
  - Not all stakeholders will be tokenholders
  - Stakeholders change over time

- Connection between a core mechanism and human input
  - Consensus itself
  - Oracles
  - Treasury Management
  - Complex Parameter Setting

Governance is not a Panacea

- Risk of Hard Forks
  - Social cost to violating credible neutrality

- Changing governance somewhere does not mean changing it everywhere

- “If the point of a blockchain is to provide a ledger of universally accepted truth, its integrity is paramount”

Insights for Regulation

- Inessential governance is likely to be competed away over time
- Data, data, data
- Principles, regulations, and code
- The dangers of DINO

Questions

Cornell Law School

DeFi and the First Law of Regulation

CFTC Technology Advisory Committee | July 2023

Defining decentralization

- In order to regulate "decentralized" financial activities, we first need to understand what we're talking about. Decentralization has several overlapping dimensions:
    - **Development** (who makes initial and ongoing design decisions)
    - **Governance** (who makes residual decisions)
    - **Operational** (who carries out decisions)
    - **Balance sheet** (who owes what to whom)
    - **Transactional** (who executes, clears, and settles transactions)
- These dimensions can be combined in different ways, in the context of different financial activities, posing different risks (but that's a story for another day).

Regulating decentralization

- An observation: existing regulatory frameworks and approaches rely heavily on a relatively high degree of *centralization* across each of these dimensions.

Identifying desired outcomes

Writing and updating rules

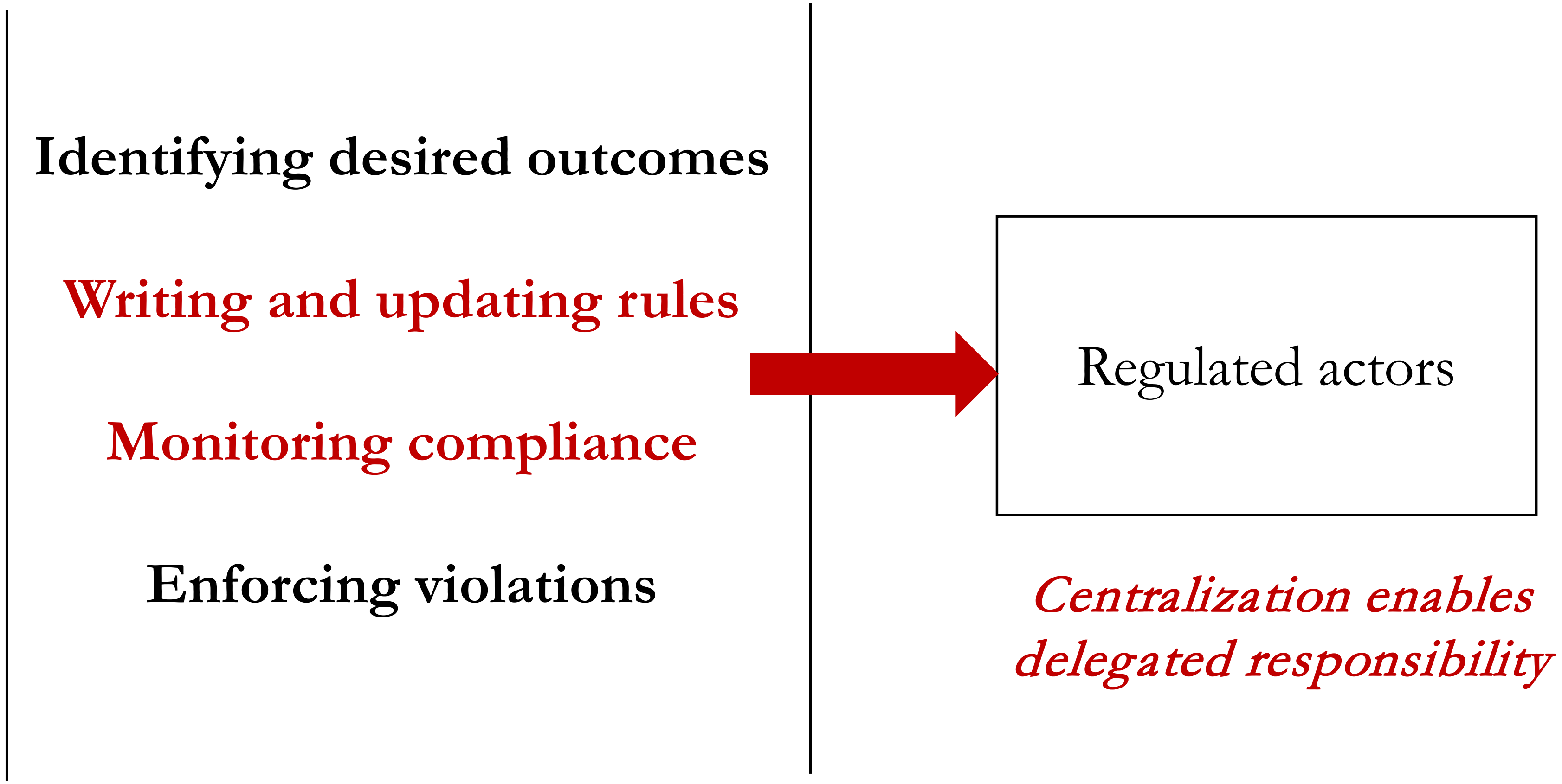
Monitoring compliance

Enforcing violations

Regulated actors

Regulating decentralization

- An observation: existing regulatory frameworks and approaches rely heavily on a relatively high degree of *centralization* across each of these dimensions.



Identifying desired outcomes

Writing and updating rules

Monitoring compliance

Enforcing violations

Regulated actors

Centralization enables delegated responsibility

Regulating decentralization

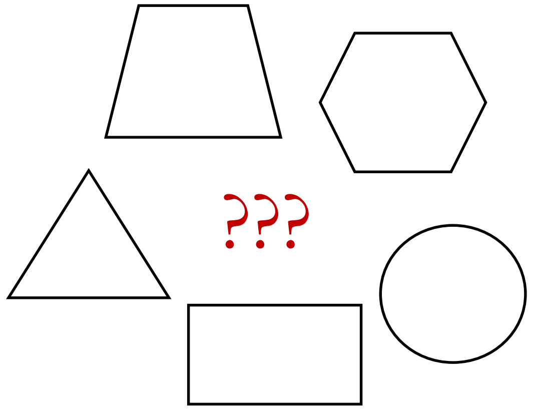
- Another observation: once we introduce significant decentralization, we need to ask whether and how these frameworks need to be adjusted in light of the **First Law of Regulation**.

Identifying desired outcomes

Writing and updating rules

Monitoring compliance

Enforcing violations



Decentralization makes delegated responsibility more complicated

Regulating decentralization

- Some questions in light of these observations:
  - How does the **regulatory *perimeter*** need to change to encompass decentralized actors and activities?
  - When, how, and on what terms should regulators ***delegate* regulatory functions and responsibility** to decentralized actors?
  - How should these functions and responsibility be **divided up *between* actors** in different decentralized financial ecosystems?
  - To what extent can regulatory functions be ***technologically* embedded** within these ecosystems? Where should they be embedded? And what role for ***humans***?
  - How can these ecosystems, and the regulatory frameworks that govern them, be made more robust to **changes in markets and regulation *over time***?

CFTC

COMMODITY FUTURES TRADING COMMISSION

Topic 3: Cyber Resilience for Financial Markets

Office of the
Comptroller of the Currency

Final Interagency Guidance on Third-Party Risk Management

CFTC Technical Advisory Committee Meeting

Kevin Greenfield, OCC

July 18, 2023

Background

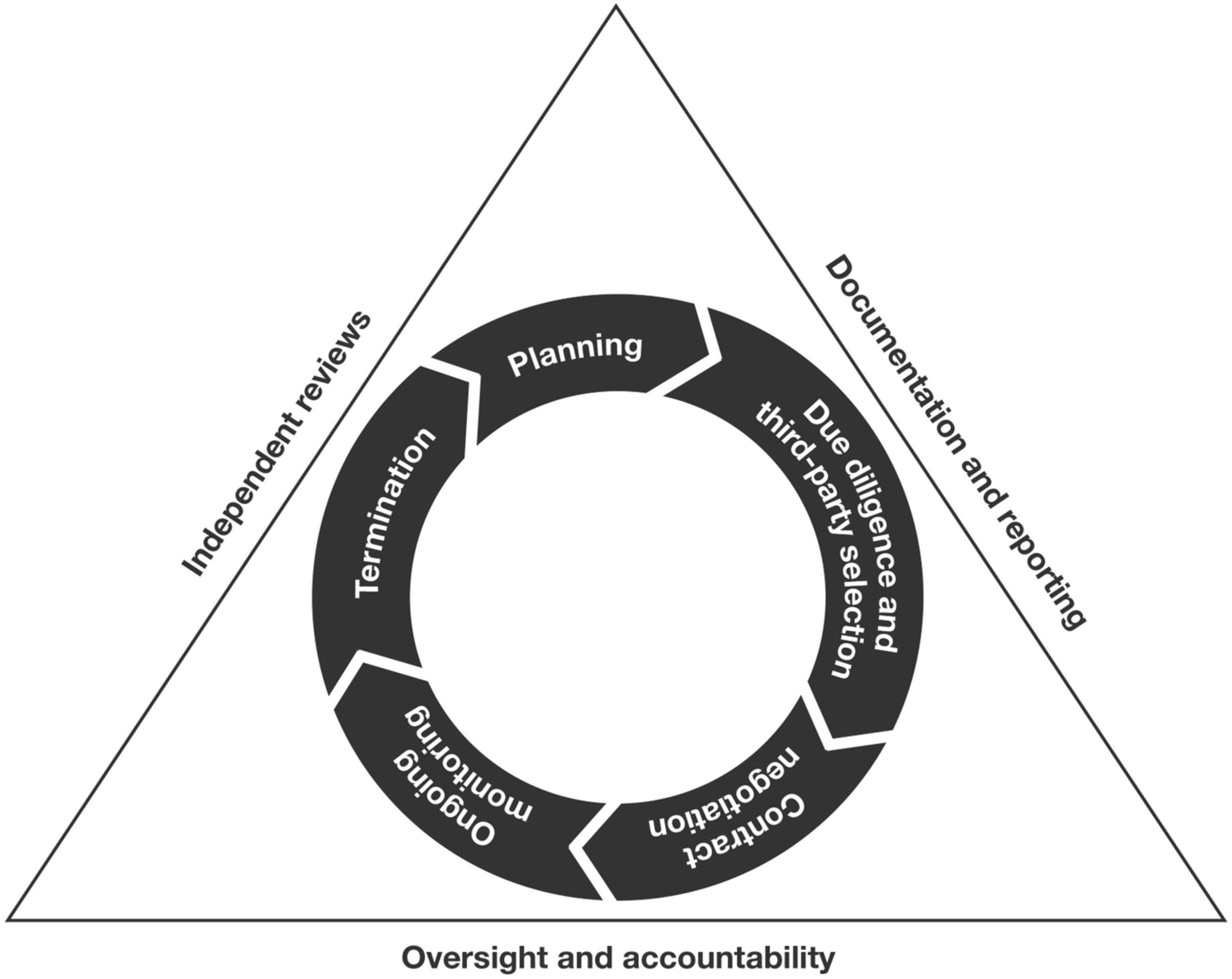
- On July 13, 2021, the OCC, Federal Reserve, and the FDIC published Proposed Interagency Guidance on Third Party Relationships: Risk Management and issued the final guidance on June 6, 2023, addressing industry feedback..

- OCC Bulletin 2023-17, “Third-Party Relationships: Interagency Guidance on Third-Party Relationships: Risk Management,” rescinds the following:
  - OCC Bulletin 2013-29, “Third Party Relationships: Risk Management Guidance”
  - OCC Bulletin 2020-10, “Third Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29”

Risk Management

- Sound risk management includes tailoring of risk management practices commensurate with:
  - the bank's size, complexity, and risk profile,
  - risks associated with services provided, and
  - the nature of the third-party relationship.
- Role of bank management and board.
- Characteristics of critical activities
- Oversight of relationships that support higher-risk activities, including critical activities.
- .Risk Management Life Cycle

TPRM Life Cycle


Planning
Due diligence and third-party selection
Contract negotiation
Ongoing monitoring
Termination
Independent reviews
Documentation and reporting
Oversight and accountability

TPRM Life Cycle Components

Component	Highlight
Planning	Activities should be aligned with the risk presented by the third-party relationship
Due Diligence and Third-Party Selection	• General approaches to due diligence. • Examples of more specific considerations (e.g., subcontracting relationships).
Contract Negotiation	• Scope and terms of contracts • Performance measures • Treatment of bank information • Operational resilience and business continuity • Subcontracting

TPRM Life Cycle Components (Continued)

Component	Highlight
Ongoing Monitoring	• Comprehensiveness and frequency based on risk and complexity of relationship. • Role of reports, testing, and visits in monitoring.
Termination	Consider ahead of time

Key Takeaways

- Each bank remains responsible for developing and implementing risk management practices commensurate with the banks size, complexity, and risk profile and with the nature of its third-party relationships.

- Banks remain responsible for their activities, whether conducted internally or through a third party.

- Principles-based guidance can assist banks develop effective third-party risk management processes.

- Banks are responsible for assessing risk and tailoring their risk management practices.

- Third-party relationships can take different forms, and the roles of the third party and the bank may differ among individual engagements.

AMERICAN UNIVERSITY
WASHINGTON
COLLEGE *of* LAW

CFTC Technical Advisory Committee Presentation:

Challenges with Understanding Cybersecurity Risk Implications for Operational Risk Regulation

Professor Hilary J. Allen

The literature on complex systems talks about the such systems being “robust yet fragile”

- Beware too much focus on efficiency and not enough focus on redundancy/ability to reconfigure in times of stress or change
- When does increasing efficiency start to be counterproductive?

Efficiency v Robustness Tradeoff

Cyberattacks get most of the attention, but:

- By some estimates, losses are greater from accidental tech glitches
- Operational threats from climate change can have similar impacts but receive less attention

Underappreciated Operational Threats

We also tend to ignore some of the systemic dimensions of operational risk

- Operational risk is typically considered as idiosyncratic to individual institutions
- That misses the possibility that operational problems can be transmitted from bank to bank through technological channels
- A "macro-operational" perspective is needed

Technological Transmission Channels for Systemic Risks

Nardello & Co.

WE FIND OUT

Trusted global investigative expertise
for today's complex world.

CFTC Technical Advisory Committee

Challenges with Understanding Cybersecurity Risk

Implications for Operational Risk Regulation

Timothy Gallagher

Managing Director and Chief Security Officer

Digital Investigations & Cyber Defense

Nardello WE FIND OUT & Co.

Threat Environment

- Cybercrime was responsible for over $10 billion in losses in 2022 (FBI – IC3)
- 300 million fraudulent signon attempts to the cloud are made every day (Microsoft)
- 53% of businesses have experienced a third party breach in the past year (Ponemon Institute)
- 60% of businesses that experience a cyber attack close their doors within 6 months (National Cyber Security Alliance)

Cyber Resilience

- Preparation
- Replication
- Recovery

Doing the Little Things Right

- Principle of Least Privilege
- Multi Factor Authentication
- Third Party Vetting
- Managed Detection & Response

FS-ISAC

Overview of Sector Cybersecurity and Risks – CFTC Technology Advisory Committee

Steven Silberstein, CEO. 18 July 2023

Who is FS-ISAC?

Mission

FS-ISAC advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve.

FS-ISAC is the **member-driven, not-for-profit organization** that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve.

Founded in 1999, the organization's **real-time information sharing network** amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defense. Member financial firms represent more than $100 trillion in assets in 75 countries.

Our Members Are:

Banks | Community Institutions | Credit Unions | Insurance Companies | Investment Firms | Financial Markets Infrastructure | Fintechs | Payment Processors | Credit Reporting Agencies | Service Providers & MSSPs

TLP WHITE

A Global Community Protecting the Global Economy

Cybersecurity is not a solo sport ▶ **No one firm can anticipate every threat, everywhere, all the time** in a digital world where every device, user, and supplier is a potential entry point for threat actors.

Cooperation yields far greater rewards ▶ But we don’t need to fight alone. While financial services is one of the world’s most competitive industries, we are also highly interdependent. **We therefore collaborate to reduce cyber risk in the sector**.

Trust is the bedrock ▶ FS-ISAC acts as a **force multiplier** of intelligence, knowledge, and practice focused on the financial sector’s cybersecurity and resilience, so that all may benefit from the experience and expertise of individual firms, no matter where they are. We can do this because we have spent nearly **25 years building a trusted community** with well-established sharing protocols.

Participation ensures our collective security ▶ Regardless of maturity and scale, **all FS-ISAC members can integrate actionable insights gained from participation** into their firm’s feedback loops for improving their own security and resilience, in turn reducing cyber risk across the global financial system.

FS-ISAC by the Numbers

Our members represent

>$100

Trillion in assets

Our intelligence exchange has

>22,000

active users

Our community is present in

5200

member firms

Our members are based in

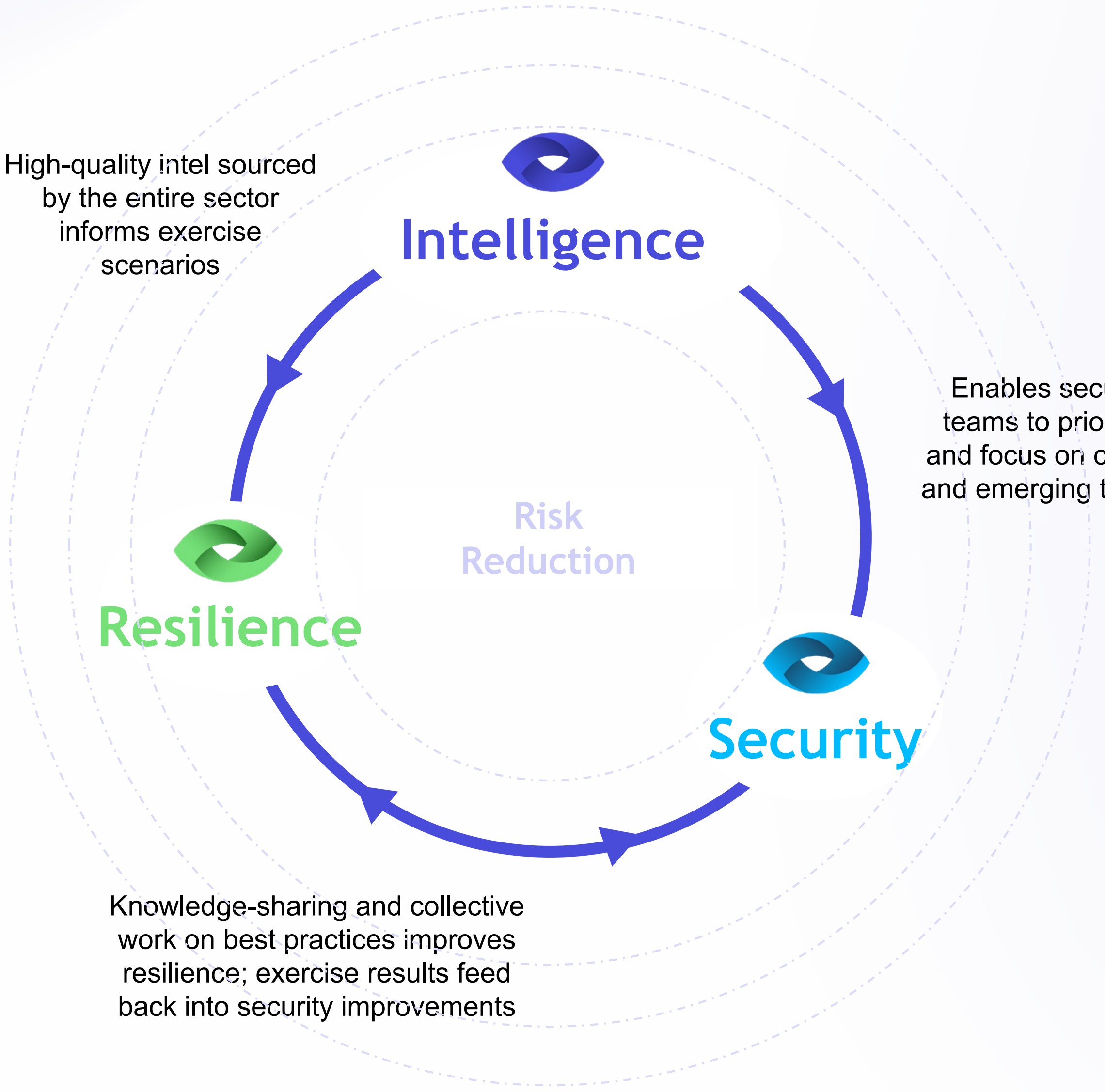
75

countries

Three Pillars of Offerings: A Virtuous Cycle of Advancing Resilience

FS-ISAC's three pillars of offerings, **Intelligence, Security, and Resilience,** allow member firms to tap into crowdsourced and enriched intelligence, security knowledge, and resilience practices to integrate into their own firm's feedback loops for reducing cyber risk.

Intelligence	Security	Resilience
▶ Sector-specific security alerting and finished intelligence analysis ▶ IntelX: member platform for accessing intel offerings ▶ Automated feeds ▶ Regional threat calls ▶ Topical/incident-focused spotlight calls ▶ Threat Intelligence Committee	▶ Trusted communities based on sub-sector, geography, functions ▶ Topical working groups ▶ Summits and regional events for knowledge sharing ▶ Community email lists ▶ Expert webinar series ▶ White papers & guides	▶ Exercises ▶ Incident response support ▶ Playbooks ▶ Critical Providers Program ▶ Business resilience committee



High-quality intel sourced by the entire sector informs exercise scenarios

Enables security teams to prioritize and focus on current and emerging threats

Knowledge-sharing and collective work on best practices improves resilience; exercise results feed back into security improvements

TLP WHITE

Resilience | Advance financial services sector resilience

Overview

Members build the muscle memory and concrete procedures to respond to attacks through exercises, training, and playbooks.

FS-ISAC coordinates sector, cross-sector, and public-private incident response to large-scale threats and enhancement of operational resilience.

Key Offerings

- **Exercises**
  - **CAPS**: on-demand, discussion-based exercises with scenarios informed by FS-ISAC threat intelligence, customized for banking, securities, and insurance sub-sectors
  - **Cyber-range:** technical, hands-on-keyboard exercises to improve tactical incident response
  - **Functional:** Act out policies and procedures at firm and sector levels in response to large-scale attack
  - **Tabletop:** Strategic discussions based on plausible scenarios with fellow members and other sector partners
  - **Cross-Sector:** FS-ISAC coordinates member participation in exercises such as NATO's Locked Shields, Tri-Sector, CyberStorm, GridEX and more.
- **Incident Response**
  - TLP Red (confidential) support for targeted organization
  - Communication channels to inform and support impacted members and wider membership as appropriate
  - One-to-many conduit for third parties to reach entire sector with real-time intelligence and mitigation advice
  - Cross-border, sector-wide, and public-private coordination during incidents
  - Development and refinement of sector-level incident response playbooks and firm-level playbook templates
- **Critical Providers Program**
  - Sector-wide insights from key sector suppliers (e.g. Akamai, Google Cloud) as well as direct, real-time communication channels during an incident
- **Business Resilience Committee**
  - Steers regional resilience efforts, helps organize and develop scenarios for regional exercises, votes on sector's current operational resilience risk level, contributes to incident response playbook.

TLP WHITE

Incident Response Case Study: MOVEit

Uniting our community to respond to a common third-party vulnerability

Global Intelligence Office Activities

- Notify all members and critical third parties who have been impacted (listed on leak site)
- Offer support into their internal investigation
  - Research on IOCs
  - Intel on threat actor (Cl0p)
- Dedicated *Connect* (secure member chat) channel with daily updated victim lists
- Briefs by Intel Office and external experts on Threat Calls

Support Security Teams

- Mitigation guidance
  - File transfer hardening guidance
- Threat hunting intelligence
  - TTPs for sprints

Act as Sector Representative

- Sharing liaison within FS-ISAC
- With governments and public-private partnership groups
- Media spokesperson

Maintaining a Trusted Community

Traffic Light Protocol (TLP)

Designations	When should it be used?	How may it be shared?
TLP WHITE	Sources may use **TLP WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	**TLP WHITE** information may be distributed without restriction, subject to copyright controls
TLP GREEN	Sources may use **TLP GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community.	Recipients may share **TLP GREEN** information with other members, trusted government and critical infrastructure partner organizations, and service providers with whom they have a contractual relationship, but not via publicly accessible channels.
TLP AMBER	Sources may use **TLP AMBER** when information requires support to be effectively acted upon, but carries risk to privacy, reputation or operations if shared outside of the organization's involved.	Recipients may only share **TLP AMBER** information with staff in their own organization who need to know or with service providers to mitigate risks to the member's organization if the providers are contractually obligated to protect the confidentiality of the information. Information can be shared with those parties specified above only as widely as necessary to act on the information.
TLP RED	Sources may use **TLP RED** when the information's audience must be tightly controlled, because misuse of the information could lead to impacts on a party's privacy, reputation or operations. The source must specify a target audience to which distribution is restricted.	Recipients may not share **TLP RED** information with any parties outside of the original recipients.

FS-ISAC Subsidiaries

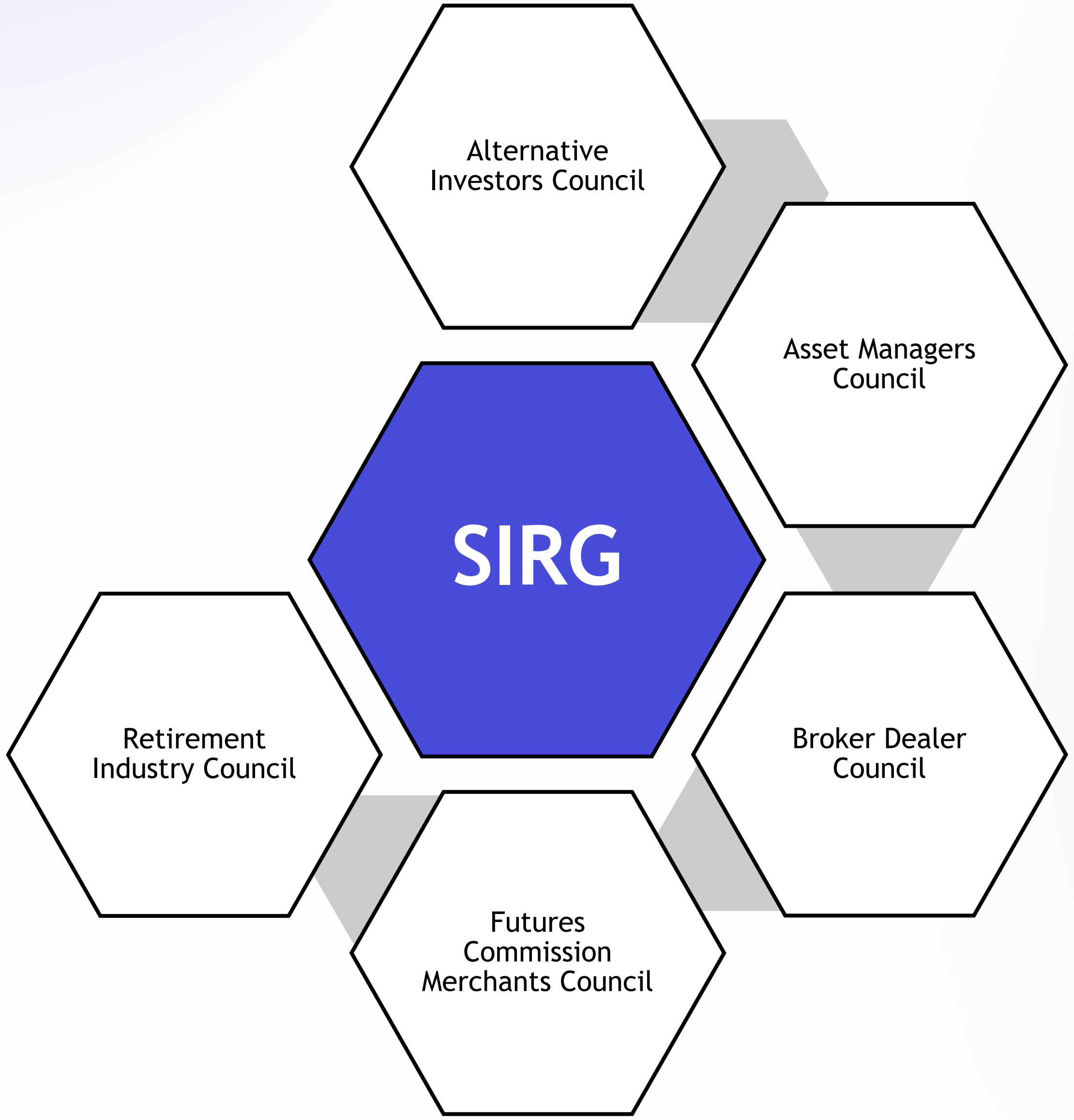
SHELTERED HARBOR

FINANCIAL™ DATA EXCHANGE

TLP WHITE

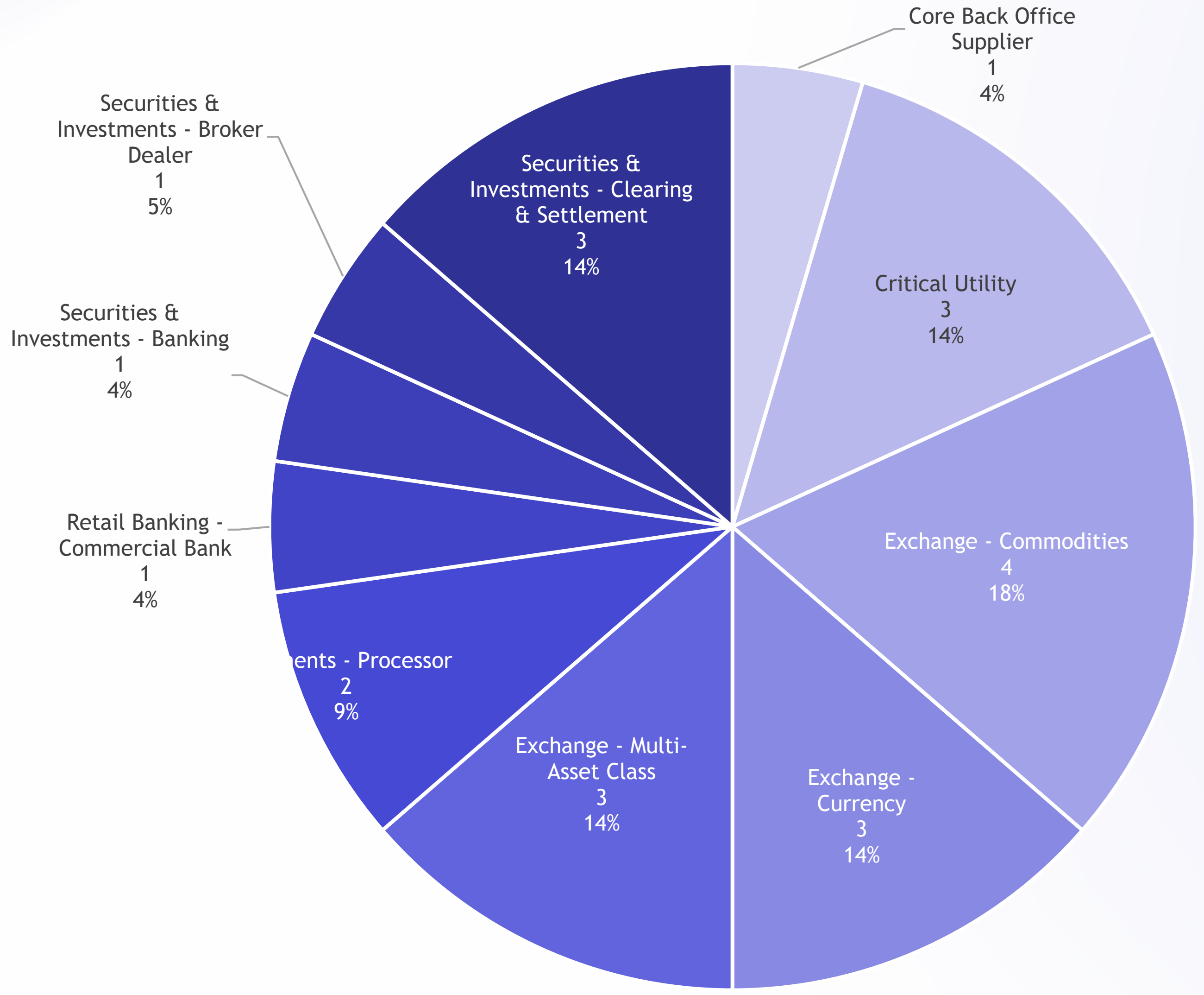
Securities Industry Risk Group

- Dedicated group for all FS-ISAC Members in the Securities & Investment Industry
- More than 1,100 Members from over 450 Firms


Alternative Investors Council
Asset Managers Council
SIRG
Retirement Industry Council
Broker Dealer Council
Futures Commission Merchants Council

The CHEF — Clearing House and Exchange Forum

- Membership from 22 clearing houses and exchanges globally
- Two geographically focused sub-groups:
  - United States - ~40 individuals
  - Global - ~24 individuals
- Strategic Initiatives include:
  - Intelligence Feeds
  - Business Resiliency
  - Employee Retention
  - Identify essential common external functions
- Incident Response unique to the needs of the CHEF
  - NZ Stock Exchange Outage due to DDOS
  - ION Trading Derivative Processing Outage



TLP WHITE

The Threat Landscape Going Forward

Vulnerabilities are continually discovered, and new exploitive technologies are constantly being deployed, so today's advanced protections become tomorrow's baseline…

- The sector's attack surface is ever expanding with the proliferation of operationally important service providers required to be competitive in a digital world.
- Customers continue to be weakest link the system and fraud/account takeover/identity theft is rising.
- The required response time for fixing published vulnerabilities is approaching zero.
- Ransomware-as-a-Service (and related attacks) still has a positive ROI although tactics are changing

Strategic Threats Need Addressing Sooner than Later

The evolving technical landscape 1-5 years out requires a long runway to implement necessary changes

- Rewiring the eco-system with quantum computing resistant cryptographic algorithms
- Ensuring Generative AI does not disrupt our Identity ecosystem
- Increasing end-user security cannot become an obstacle for the digitally challenged
- MDM (mis/dis/mal information) can erode the trust of our institutions

TLP WHITE

The Sector has Collaborated on It's Core Resiliency…

With Public-Private-Partnerships to foster resiliency, incident response and supply chain security:

- Key FBIIC-FSSCC Collaborations:
- The sector-wide "All Hazards Playbook" and CERG (Core Executive Response Group) was stood up for COVID-19 on 30 Jan 2020, and continued to operate through Solar Winds to the Russia/Ukraine Invasion.
- Hamilton Exercises continue to advance the learnings on new and unexpected events
- ION Trading outage demonstrated good collaboration between CFTC/FBIIC/FIA/FS-ISAC/SIFMA
- Cloud Security Workstreams – Public Sector/Private Sector/Joint projects
- Critical Functions Definitions

FS-ISAC’s Supply Chain Efforts

- Created a unique “Critical Provider Program” for mission critical suppliers
- “Software Supply Chain” Working Group focused on SBOM adoption
  - Encouraged Back-Office suppliers and Payment Processors to join
- Leading one of the FSSCC Cloud Work Streams on resiliency
- Evolving our CAPS exercises to sub-sector specific scenarios for better training
- Investing in our Business Resiliency Community of Interest

TLP WHITE

Thank you

CFTC

COMMODITY FUTURES TRADING COMMISSION

Closing Remarks