Speaker A
Speaker B

Slide 1
A
"Good afternoon. Today we will be showing our final project about crypto scams. Imagine a $1.3 billion industry—in 2021 alone, cryptocurrency frauds cost that much. This is about harmful data patterns that can be recognized and prevented, not only bad criminals.
A
Our project focuses on transforming this complex challenge into a solvable programming problem. We didn't just study scams; we analyzed the digital trail they leave behind to build a predictive defense mechanism.

Slide 2
B
How can a single exchange or regulation proactively detect and report new, clever cryptocurrency frauds before they result in significant financial loss? This is the main business issue we explored.
Two crucial analytical questions resulted from this:
B
Is there a measurable difference in the transactional behavior of fake and authentic cryptocurrency wallets?
B
Can we effectively train a machine learning model to reliably identify new cryptocurrency entities as "Scam" or "Legitimate"?

Slide 3
A
"Let's examine the complex nature of the data itself before delving into our techniques. Anonymity and low barriers to entry are the main causes of the abundance of cryptocurrency frauds, ranging from straightforward phishing to sophisticated smart contract exploits and outright investment scams.
B
Anonymity in Code: By making small changes to outdated, dangerous smart contracts, blockchains enable con artists to swiftly iterate and implement new scam subcategories. They can quickly create a new strain by simply changing the tokenomics or renaming a function if a "Rug Pull" template is recognized.
A

Market Volatility: The quick emergence of new cryptocurrency niches, such as NFTs, DeFi loans, and meme currencies, provides scammers with fresh opportunities. There is a new attack surface for each new feature on the blockchain.

Slide 4

B

"Powerful insights into the composition and frequency of these scams were instantly revealed by our feature engineering and preliminary analysis. We'll examine two crucial visuals that reinforced our modeling strategy.

A

📊 Scam Frequency: Analysis of Attack Vectors

[See Pie Chart: Scam Subcategory Distribution]

The distribution of scam subcategories in this pie chart illustrates the areas where users are most at risk. Two categories clearly dominate: MyEtherWallet at 28.6% and Trust-Trading at 34.5%.

A

Trust-Trading is an example of a purely social engineering approach in which con artists use the promise of large rewards to persuade victims to transmit money. Its high percentage demonstrates that the biggest attack vector is still human susceptibility.

Slide 5

A

"Our study revealed that just two major types accounted for over 63% of the subcategories in our dataset: MyEtherWallet (MEW) Impersonation at 28.6% and Trust-Trading at 34.5%. A

The Social Attack: Trust-Trading

Trust-Trading is a pure social engineering fraud in which victims are convinced to transmit bitcoin by promises of enormous, risk-free profits. This high percentage demonstrates that trust is still the biggest weakness.

B

Examining the operational structure under the 'Scamming' category in our box plot reveals that these operations frequently entail a greater number of connected addresses. This is the scammer's operational footprint; they utilize these dozens of locations to swiftly distribute and launder money through layering, making it very challenging for forensic teams to track them down.

B

The Infrastructure Attack: MyEtherWallet Impersonation

MEW impersonation is an infrastructure-based scam that is often categorized as a phishing attack. Scammers use virtually identical phony MEW websites to deceive users into signing dangerous transactions or entering their private keys.

Our box plot analysis for the 'Phishing' category shows a similar trend to 'Scamming,' indicating a large network of associated addresses is also required here. This network isn't just for laundering; it represents the infrastructure—the disposable drop wallets, the numerous domain-squatted sites, and the automated scripts needed to run a sophisticated, high-volume phishing campaign.

These two types of scams, one targeting social trust and the other targeting site trust, required a model that could identify both the small, high-value transfer signature of Trust-Trading *and* the large, distributed network signature of Phishing. This informed our final predictive approach.

Slide 6
B

"The key insight from our project is that effectively avoiding crypto scams requires a multi-layered defense strategy that protects the code, the user, and the exchange platform itself.

How to Avoid Scams

We've broken down prevention into two levels, corresponding to the analysis we performed:

1. Programmer/Developer Level (Targeting our Model's Features):
    - Audit Early and Often: Integrate static analysis tools in the CI/CD pipeline. These programming tools flag suspicious transactional features—like rapid token dispersion—*before* a contract goes live.
    - Prioritize Recall: When deploying our classification model, security teams must configure the system to prioritize high Recall, accepting a few false positives to ensure zero high-value scams slip through.
2. User Level (Targeting Trust-Trading and Phishing):
    - Verify Website URLs: To combat MyEtherWallet impersonation, always manually type the URL or use bookmarked links. Never trust links sent via Telegram or DMs.
    - Trust No One: To avoid Trust-Trading scams, remember that legitimate projects never ask you to send funds directly to a personal wallet address for a guaranteed return. If it sounds too good to be true, it violates the basic principles of secure finance.

This leads us to our final conclusion, summarizing the importance of our project's approach."

Slide 7
A

"The true value of our project lies not just in the model's accuracy, but in the key insight it validated: Crypto scam defense must be a multi-layered strategy that protects the code, the user, and the platform.

Our model confirmed that scammers exploit both technical timing and human trust. Therefore, avoiding future scams requires parallel solutions:

Defense at the Programming & Platform Level

For developers and exchanges, the takeaway is clear: prioritize vigilance based on feature importance.

- Audit for Temporal Signatures: Since our model showed Wallet Age and Activity Volatility are the most predictive features, platforms must aggressively flag and investigate any new token or contract that exhibits rapid creation followed by a single, massive fund consolidation—the classic profile of a Rug Pull.
- Prioritize Recall: When deploying our classification model, security teams must configure the system to prioritize high Recall (catching actual scams), accepting a few false positives to prevent catastrophic losses.

Defense at the User Level

To combat the dominant Trust-Trading and MyEtherWallet Impersonation scams we analyzed:

- Assume Zero Trust: Never send funds to a personal wallet address based on a guaranteed return; this is the core mechanism of the 34.5% Trust-Trading scams.
- Verify the Source: Manually type the wallet or exchange URL and check the security certificate. This is the simplest defense against the 28.6% of scams stemming from Phishing and Impersonation.

Slide 8

B

To conclude, we began our project with a complex problem: the relentless growth of crypto scams, driven by both technical vulnerabilities and human error.

B

Through rigorous data analysis and programming, we successfully engineered features that capture the unique behavioral signatures of major scams like Trust-Trading and MyEtherWallet Impersonation. We then validated these findings by training a [Insert Model Name] capable of predicting fraudulent activity with a strong Recall score of [Insert Recall Score].

A

Our core finding is that effective security is not a single tool, but a robust system. By prioritizing our validated features, platforms can shift from *reactionary* recovery to *proactive* defense.

The financial reality is simple: The cost of implementing a data-driven, multi-layered security system is exponentially less than the cost of a single, successful, multi-million dollar scam.

We hope our work provides a solid framework for how cybersecurity programming and data science can defend the decentralized future.

B

We invite you to explore our full methodology and code. You can find our complete notebook and GitHub repository link here on the final slide.

Thank you for your time.