FIDES

WHAT HAPPENS IN BLOCKCHAIN, STAYS IN BLOCKCHAIN.

Receive updates instantly

JOIN OUR NEWSLETTER

Enter your email address | Subscribe Now

$1.9B

This year $1.9B has been lost to hacks. Of this, 45% of hacks are from code-related exploits. Hundreds of millions are lost every year due to a lack of security - we plan to stop this.

OUR INSIGHT

Protection happens at the wrong time

Existing solutions focus on pre-hack mitigations or post-hack recoveries. Both methods are incomplete prehack solutions don't know what the hack will look like, and post-hack solutions can't undo damages. We realized that you can act in the window of time between a hack's proposal to the mempool and its acceptance on-chain. This way, you get access to information and can still block the hack. Our solution involves detecting hacks as they happen before they have time to damage the target contract.

PIPELINE

1 Monitor for Incoming Transactions

To defend protocols from incoming hacks we need to know about the transactions before they're added on-chain. We do this by monitoring the public mempool and by forming partnerships with private mempools. With the help of Flashbots, we're building a modified version of GETH that can be used by private mempools to notify us of anomalous transactions.

On non-ETH chains, our strategy will differ based on the architecture. On Binance, for example, we'd work directly with the 21 validators to detect incoming hacks.

2 Detect Malicious Transactinos through Anomaly Detection

To determine whether a transaction is malicious or not we use anomaly detection models. These models have been trained to know what normal activity looks like on each monitored contract. When they see something out of the norm, they asume that it's a hack and trigger our defense strategies.

3 Defending Protocol Users

To defend protocols from incoming hacks we have two options;

1. Firstly, we can pause the contract. This will stop the hack in its tracks but is also disruptive to protocols in cases where we detect false positives.
2. Secondly, we can take the incoming transaction, modify it, and white-hat hack the at-risk protocol. This way protocols don't need to trust us with any permissions. It also minimizes the disruption of false positives since we're only able to hack the protocol if it was at risk.

TECHNICAL STRATEGY

Data Collection

To train our models, hundreds of thousands of benign transactions are required. We collected 50 contracts that have been hacked and scraped data on all their internal transactions.

Data Representation

From our datasets of transactions, we extract features including the opcode, events, interacted contracts, etc. We also extract hand-crafted features like whether a given user was funded by Tornado Cash.

Hack Detection

We found that anomaly detection is a fantastic proxy for finding hacks. We've put together a set of unsupervised models that achieve an 80% true positive rate and a 0.02% false positive rate. To be commercially viable we plan to reduce the false positive rate by one to two orders of magnitude. Right now we're looking into generalizable models and larger datasets to help push it down!

True Positive Rate: 80%

False Positive Rate: 0.02%

MARKET STRATEGY

White-Hat Hacking

For protocols that don't want to give us access to their pause function, we can still protect them. We'll modify the hack transaction and white-hat hacking them, moving the funds to a pre-diced address

We will monetize this strategy by taking a bounty 5-10% TVL upon defending a protocol's funds. This way, protocols will only ever play when they used our service.

Pausing Protocols

For protocols that allow us access to their pause function, we can defend them by halting their contracts upon detecting a hack. This solution covers more kinds of hacks but also introduces the risk of false-positive events.

We will monetize this strategy by charging protocols a yearly fee for our service. This is similar to a proposal accepted by Aave last year, where Certora offered continuous formal verification for $3.4M / year.

OUR TEAM

Robert MacWha - Co-Founder & CEO

ML engineer with 5 years of experience. Project manager on consulting challenges for Shell and the United Nations. Previously @Aspire.

Dickson Wu - Founder & CTO

ML engineer with 3 years of experience. Founding member of PadawanDAO, previously @Rapyuta Robotics, @Spectral Finance.

Robert MacWha - Co-Founder & CEO

ML engineer with 5 years of experience. Project manager on consulting challenges for Shell and the United Nations. Previously @Aspire.

ADVISORS ET INVESTORS

Goncalo Sa Co-Founder (ConsenSys Diligence) Angel Investor	**Alex Svanevik** CEO (Nansen) Angel Investor	**Daniel Von Fange** Security Researcher (Origin Protocol) Advisor	**Hickup** Smart Contract Auditor (CodeArena) Angel Investor
Nootrality Co-Founder (MTTrispect) Advisor	**Hudson Jameson** Core Ethereum Developer Angel Investor	**Duncan** Investor (FoodCapital) Angel Investor	**Dorahacks** investor

TIMELINE

Seed Raise
Raising $1.1M at an $11M valuation to support us for the next 18 months.

Development
Developing our protocol protection service.

Trials
Testing our models with real-time data to verify their accuracy.

Multi-chain
Expanding to secondary chains like Optimism, BSC, and Solana.

SEED ROUND

$1.1M Raise

In our seed round, we're raising $1.1M, representing a monthly outflow of $60k for 18 months. This monthly outflow accounts for 5 engineers to build this full-time.

We plan to raise at an $11M pre-money SAFE round. So far we've had >$500k in commits from angel investors and funds.

Our Vision

While we're currently only working on stopping hacks in real-time, we plan to expand into other security areas in the future. ML-powered auditing, on-chain protections, and defenses against fraud are all areas that we hope to expand into as we grow as a company.

Overall, we plan to secure the Web3 industry.

ONE LAST THING

Vitalik's Favourite Project

At EthDenver2022 we were Vitalik's favorite project and placed third in the community vote!

Binance MVB Incubator

We were selected from 650+ applicants to participate in Binance's MVB incubator program.

FIDES

JOIN OUR NEWSLETTER

Enter your email address | Subscribe Now

CONNECT WITH US