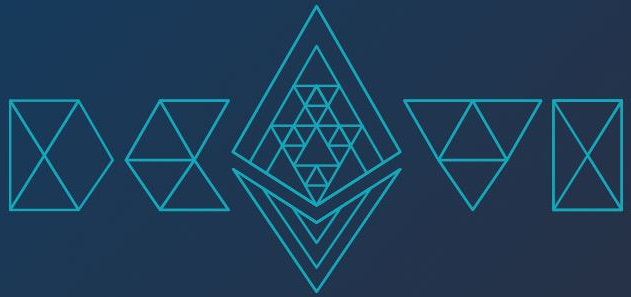


The $10B Problem

Web3 Security Against Coordinated Adversaries

Julia Hardy and Adam Hart
Chainalysis

Chainalysis: A Blockchain Analytics Company

DATA INPUTS

- Blockchain Data
- Proprietary Research
- Cryptocurrency Exchange Data

DATA PREP STEPS

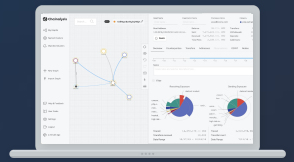
Normalize
Standardize storage and labelling across blockchains

Clustering
Group addresses controlled by the same entities

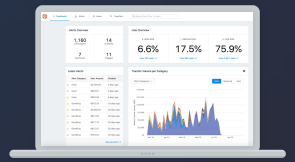
Attribution
Assign labels to identified entities

Enhancement
Algorithms run on labelled data for greater coverage

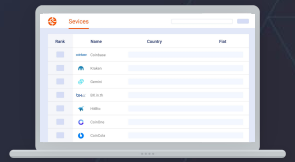
REACTOR



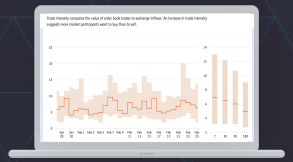
KYT



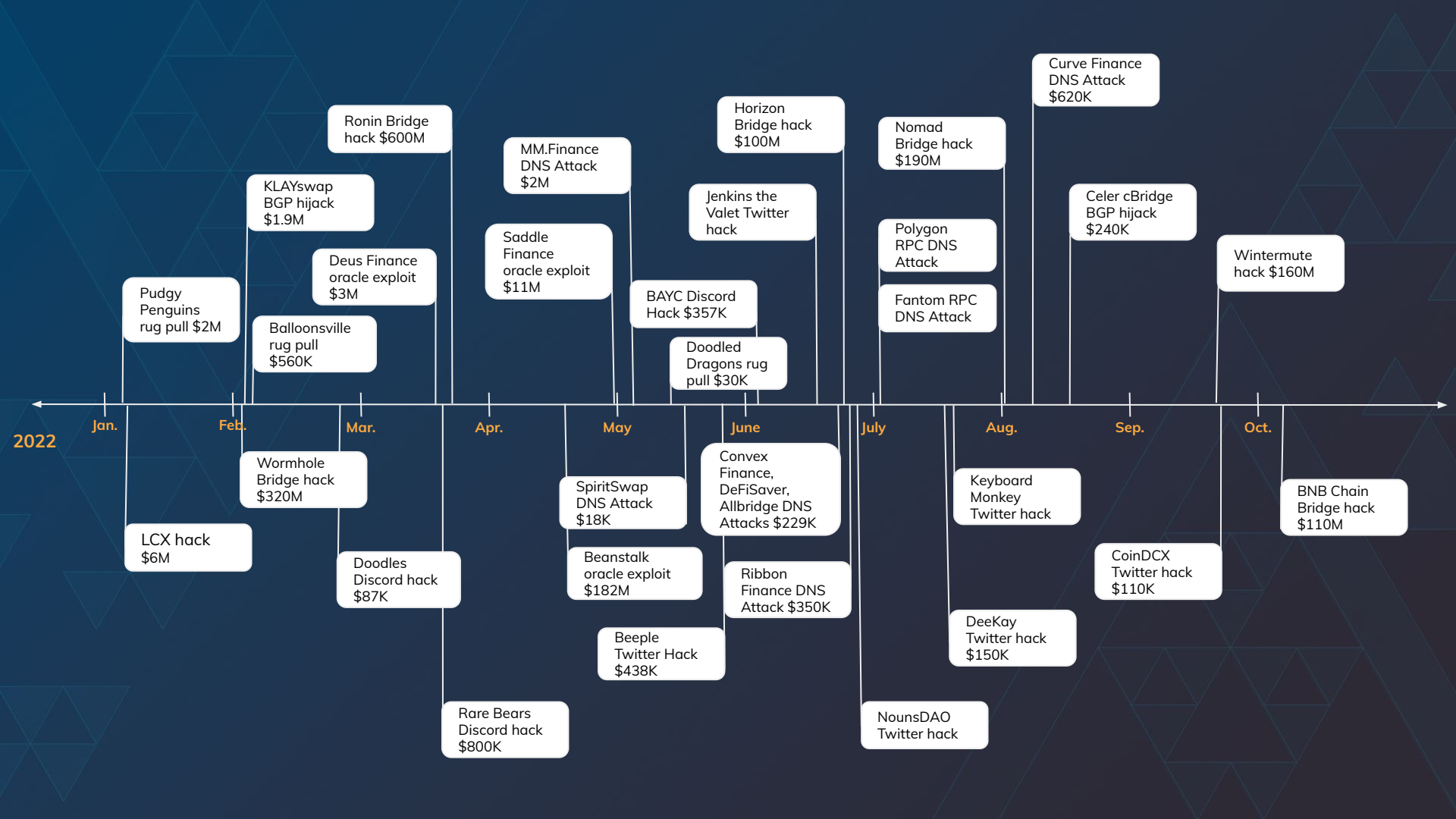
KRYPTOS



MARKET INTEL



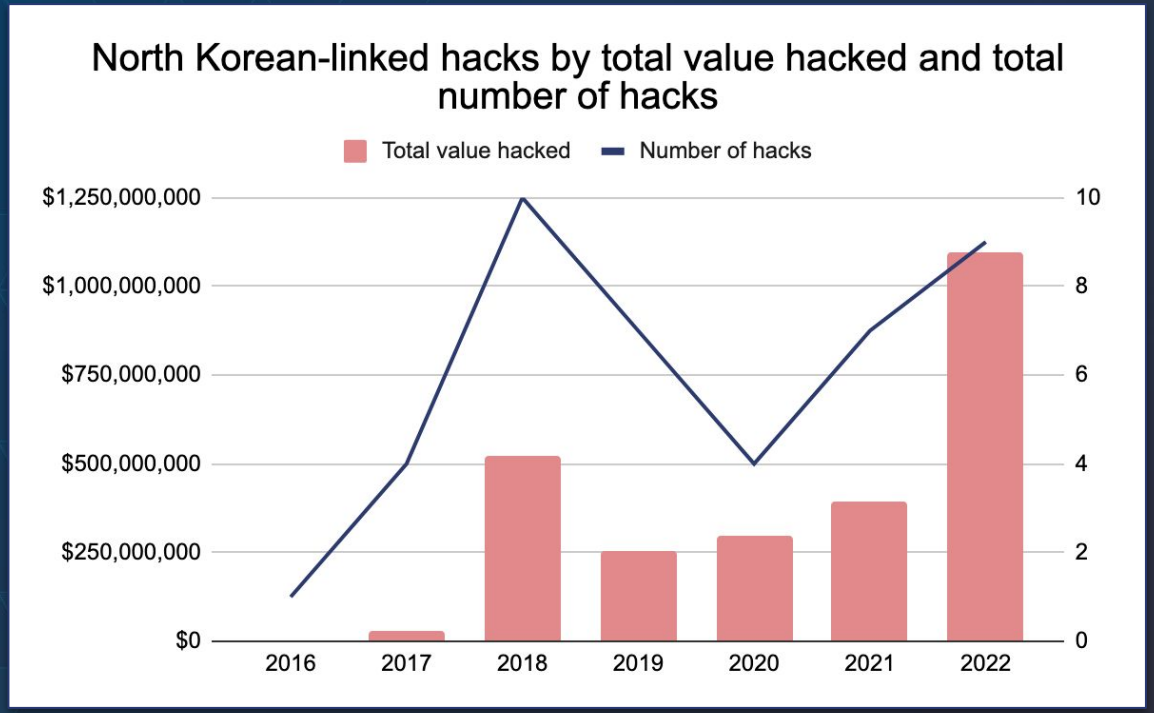
Chainalysis


2022
Jan.
Feb.
Mar.
Apr.
May
June
July
Aug.
Sep.
Oct.
Pudgy Penguins rug pull $2M
LCX hack $6M
KLAYswap BGP hijack $1.9M
Wormhole Bridge hack $320M
Balloonsville rug pull $560K
Deus Finance oracle exploit $3M
Doodles Discord hack $87K
Ronin Bridge hack $600M
Rare Bears Discord hack $800K
Saddle Finance oracle exploit $11M
MM.Finance DNS Attack $2M
SpiritSwap DNS Attack $18K
Beanstalk oracle exploit $182M
Beeple Twitter Hack $438K
BAYC Discord Hack $357K
Doodled Dragons rug pull $30K
Jenkins the Valet Twitter hack
Convex Finance, DeFiSaver, Allbridge DNS Attacks $229K
Ribbon Finance DNS Attack $350K
Horizon Bridge hack $100M
NounsDAO Twitter hack
Nomad Bridge hack $190M
Polygon RPC DNS Attack
Fantom RPC DNS Attack
Keyboard Monkey Twitter hack
DeeKay Twitter hack $150K
Curve Finance DNS Attack $620K
Celer cBridge BGP hijack $240K
CoinDCX Twitter hack $110K
Wintermute hack $160M
BNB Chain Bridge hack $110M

Section 1

Nation State Adversaries

Chainalysis has identified 42 DPRK hacks since 2016



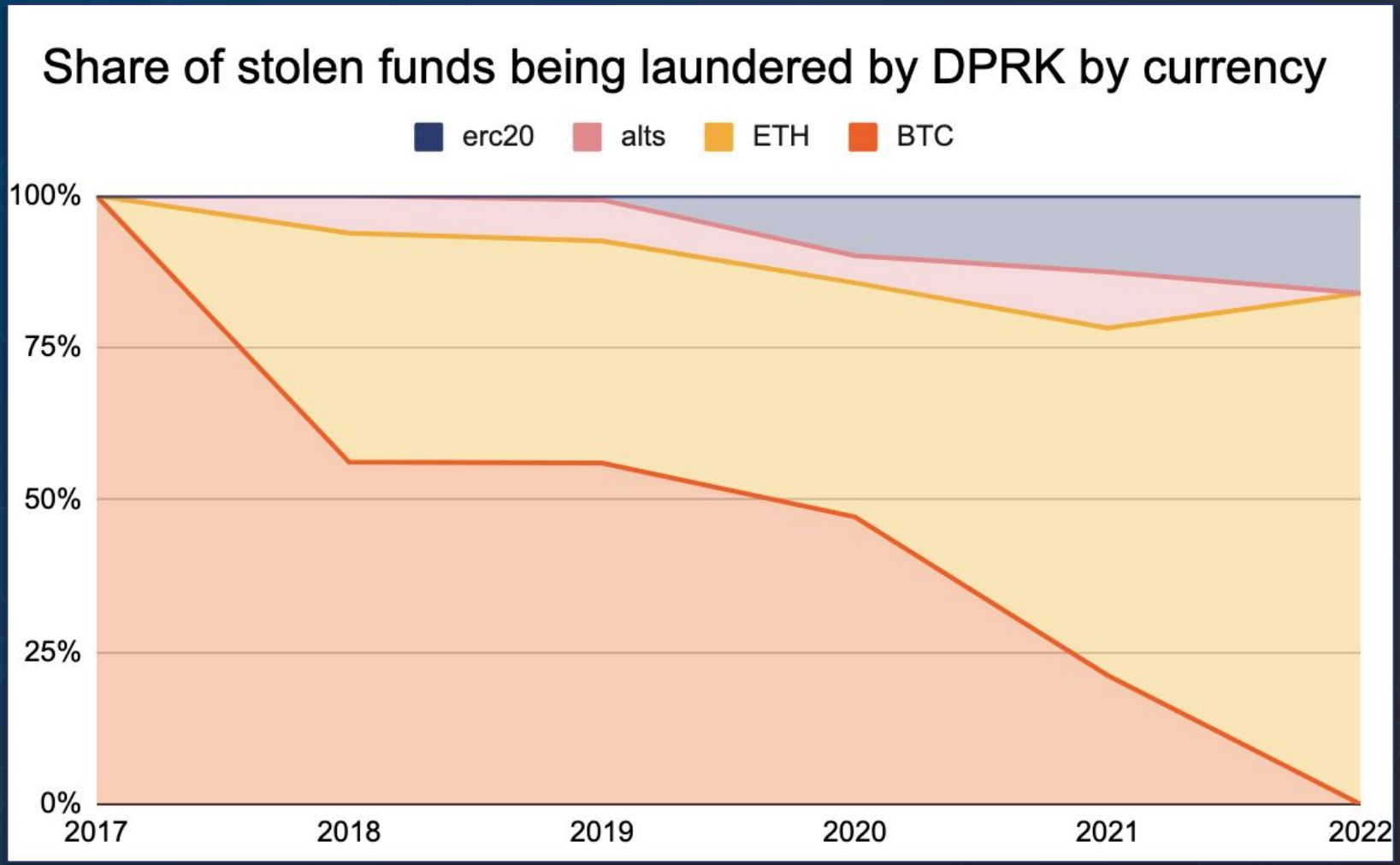
~$2.7B hacked funds investigated

Kucoin largest hack in 2020 - $275M stolen

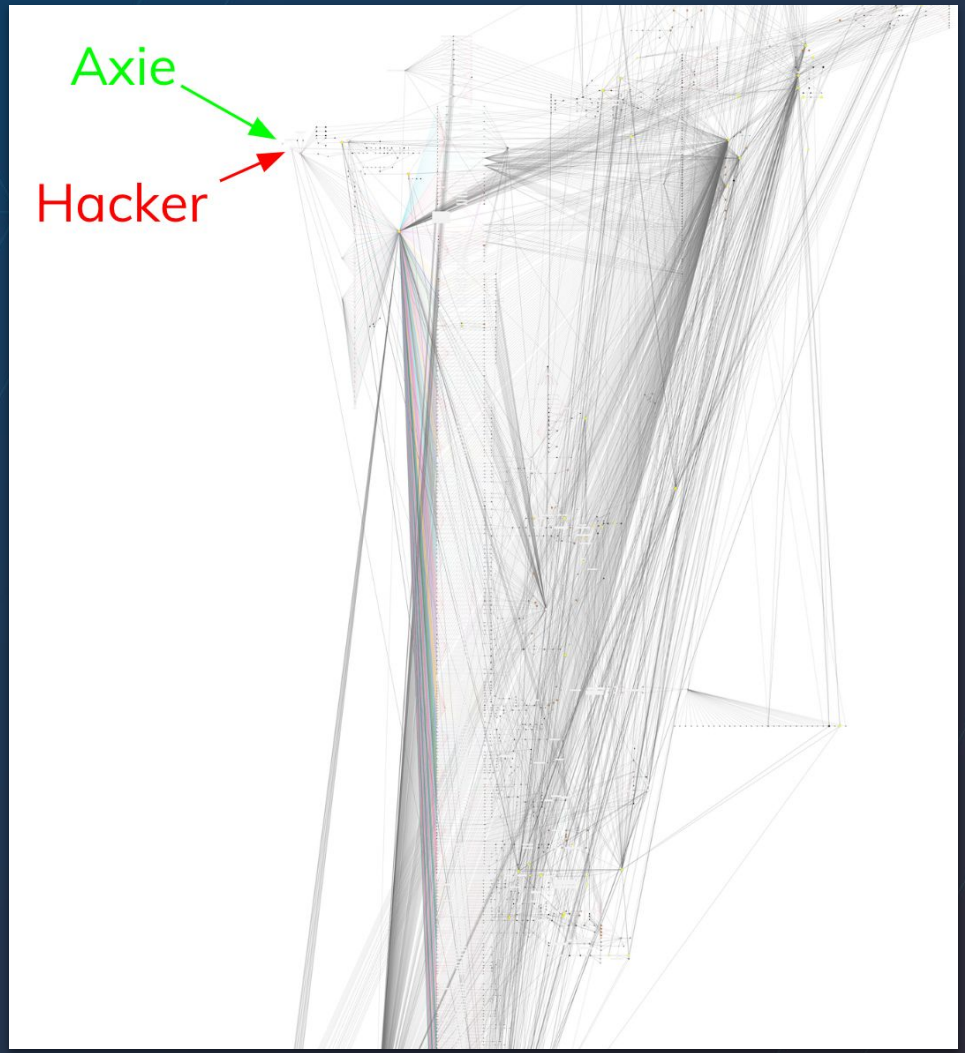
Ronin hack - biggest single hack to date

~30% of all hacked value went to DPRK since 2017

https://go.chainalysis.com/2021-Crypto-Crime-Report.html



https://go.chainalysis.com/2021-Crypto-Crime-Report.html


Axie
Hacker

Section 2

Lazarus Is Not The Only Coordinated Adversary

Compromised dapp front ends via vulnerable web2 infrastructure

QuickSwap
@QuickswapDEX

⚠️DO NOT SWAP⚠️

Similar to other protocols hosted on @GoDaddy, QuickSwap has been domain hijacked

Funds in LPs, the Dragon's Lair, Syrup Pools, & YOUR wallets are safe

Only swaps have been affected. Please DO NOT SWAP

BORDER GATEWAY PROTOCOL INSECURITY —

How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000

For 2nd time in 4 years, Amazon loses control of its IP space in BGP hijacking.

DAN GOODIN - 9/23/2022, 1:04 PM

Compromised Discord servers

Bored Ape Yacht Club
@BoredApeYC

Our Discord servers were briefly exploited today. The team caught and addressed it quickly. About 200 ETH worth of NFTs appear to have been impacted. We are still investigating, but if you were impacted, email us at discord@yugalabs.io.

3:16 PM · Jun 4, 2022

OpenSea Support
@opensea_support

We are currently investigating a potential vulnerability in our Discord, please do not click on any links in the Discord.

3:43 AM · May 6, 2022 · Twitter Web App

Identifying Coordinated Campaigns

Off-chain analysis

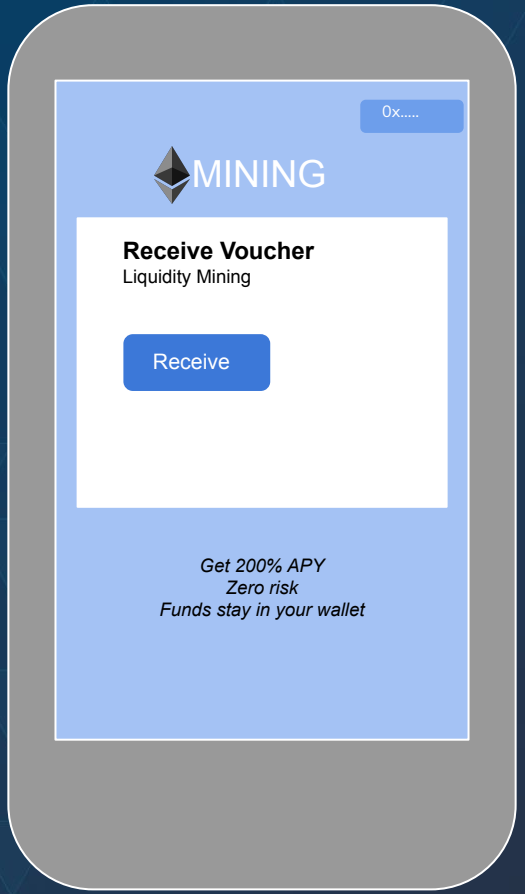
- Traditional incident response analysis
- What system was compromised?
- How was that system compromised?
- Infrastructure used

On-chain analysis

- What is the payload?
  - Token approval phishing
  - Seed phrase phishing
  - Eth_sign phishing
- Fund movement post attack
  - Consolidation of funds pre/post mix
  - Distinctive laundering patterns

Section 3

Case Study: USDT Approval Mining Scam



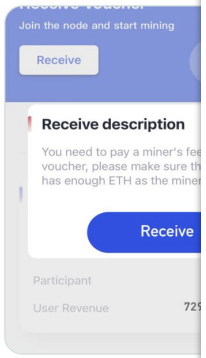
MetaMask @MetaMask

⚠️ PSA: There's a new scam making the rounds - fake "mining" sites that ask you to join a "node."

The site will attempt to connect to your wallet and get you to approve unlimited access to your tokens.

So far, they seem to be targeting mobile users & their $USDT.

1/ 🧵

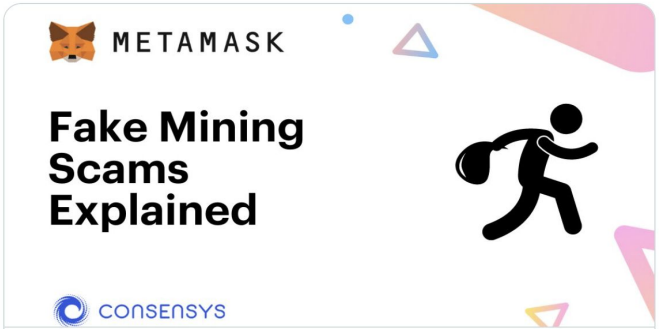


2:40 PM · Mar 29, 2022 ·

ConsenSys @ConsenSys

If you've kept up to date with our various Twitter handles, you'll know we can't talk enough about token approval scams – a new format, observed by @sniko_ and others on our team, involves sites offering 'mining' rewards ⛏️

1/6



consensys.net
Fake "Mining" Scams: a Familiar Foe in a New Disguise | ConsenSys
An increasingly common scam uses token approvals to steal tokens whilst suggesting you're earning yield on them

12:44 PM · Jun 28, 2022 · Twitter Web App


mining-scam.com
Apply rewards
Root Address
0x
Actions
Balance: 0.00 USDT_ETH
Sent: 14,982 USDT_ETH
Received: 14,982 USDT_ETH
Total Fees: 0.00 USDT_ETH
Record
Function: transferFrom(address _from, address _to, uint256 _value)
MethodID: 0x23b872dd
[0]: 000000000000000000000000b1da8a5ae0b19f2e800befd3d541b4e0954e57eb
[1]: 000000000000000000000000628db722c3804849947e04431f773a73c0331d69
[2]: 0000000000000000000000000000000000000000000000000000000000245737a43

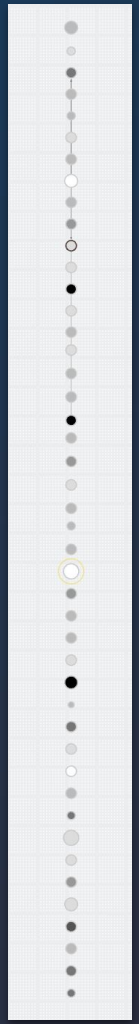
60+ scammer addresses reported

~$83M reported stolen
from October 2021 to October 2022

Identified off-chain coordination, including use of the same domains and a focus on mobile users

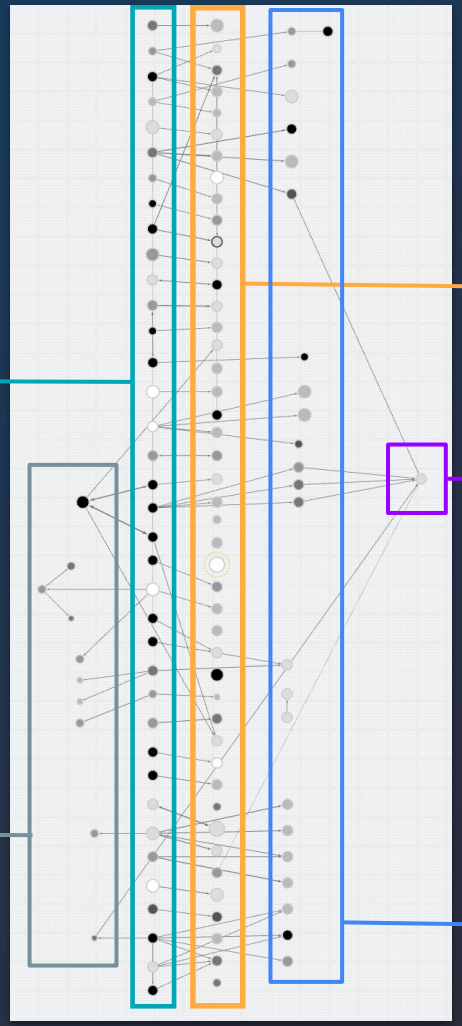
Created Dune Analytics dashboard to make reported information publicly available

Reported Scammer Addresses



Dune Analytics

Identifying Patterns



Initial gas funding

Reported scam addresses granted approval to move victim tokens

Consolidation point

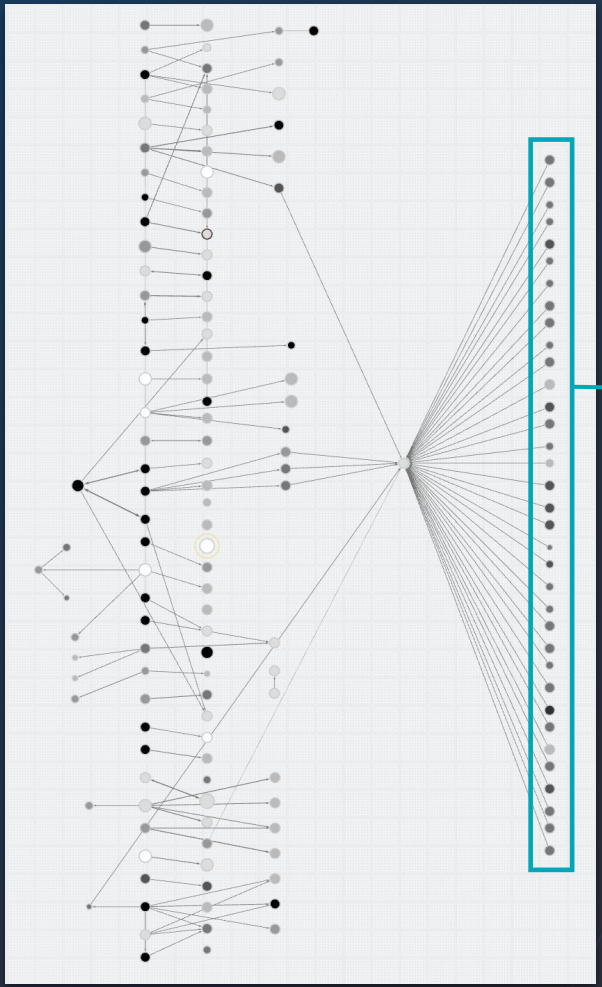
Observed phishing script testing pattern

Additional addresses receiving victim approvals

Mapping The Scam Network

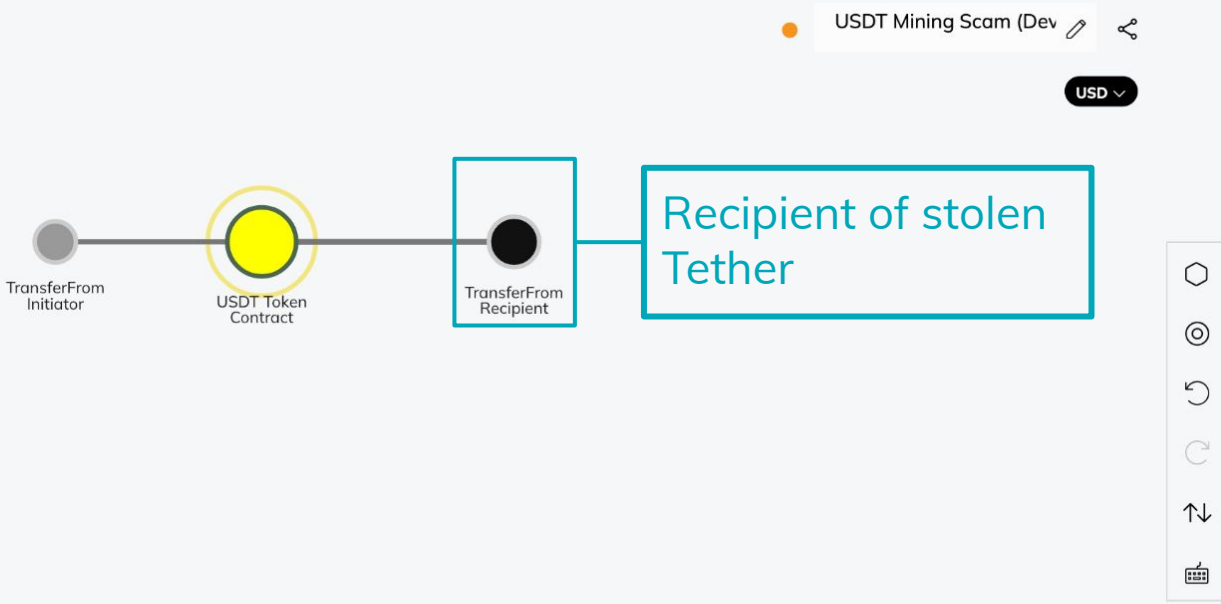
Identified addresses

- **91** addresses phishing for approvals from victims
- **879** addresses receiving likely victim funds via transferFrom
- **>11,000** new potential victim addresses

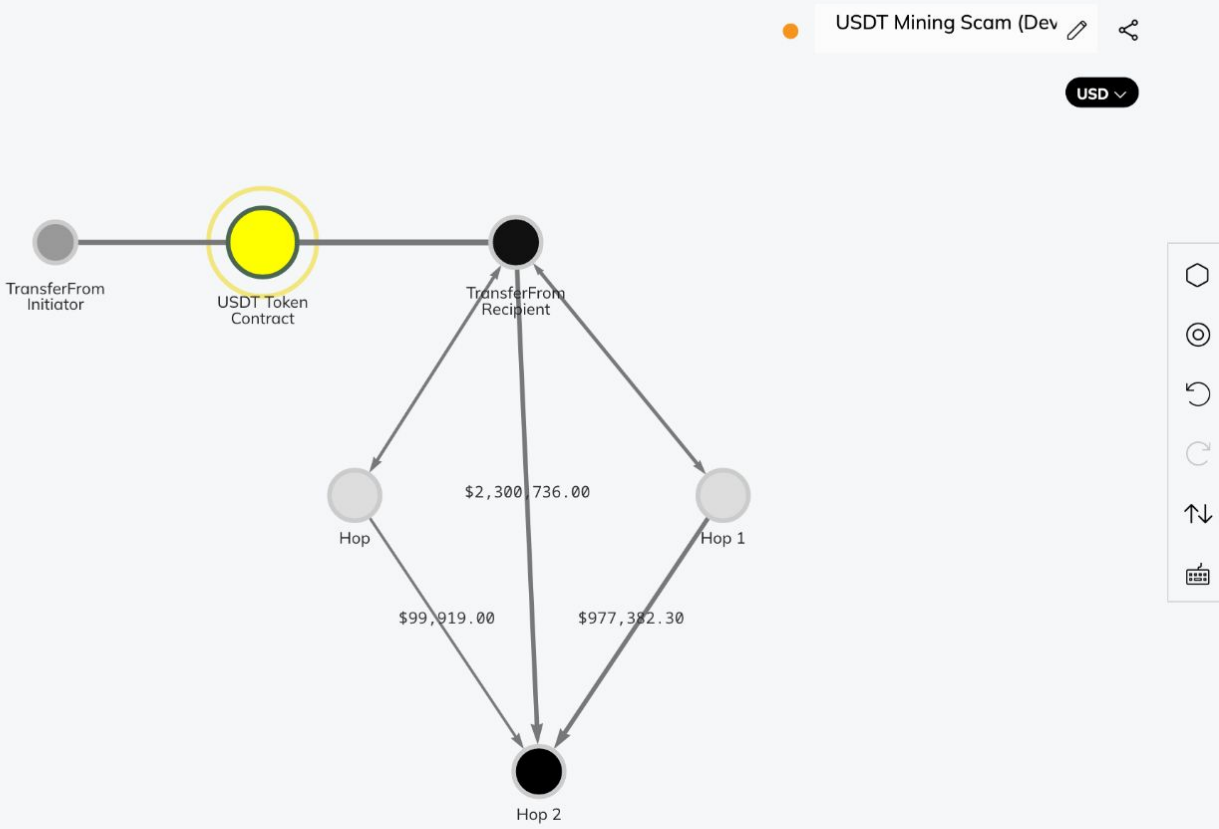


Newly identified addresses receiving token approvals from victims

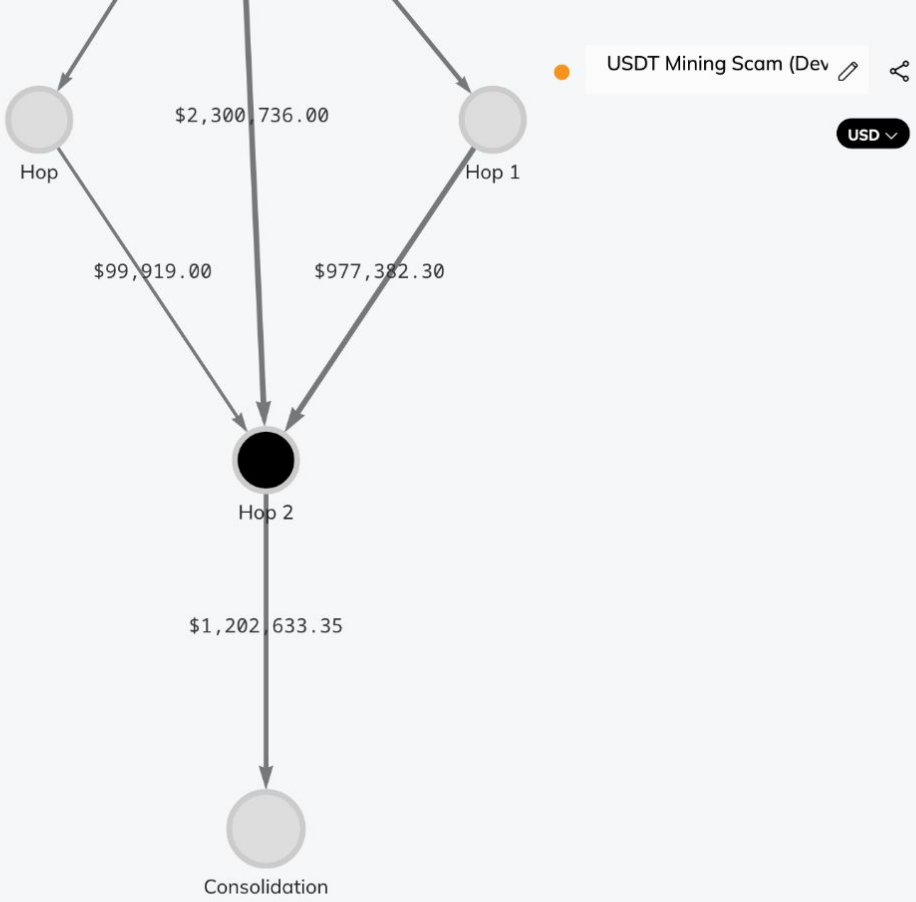
Recipient of Stolen Tether



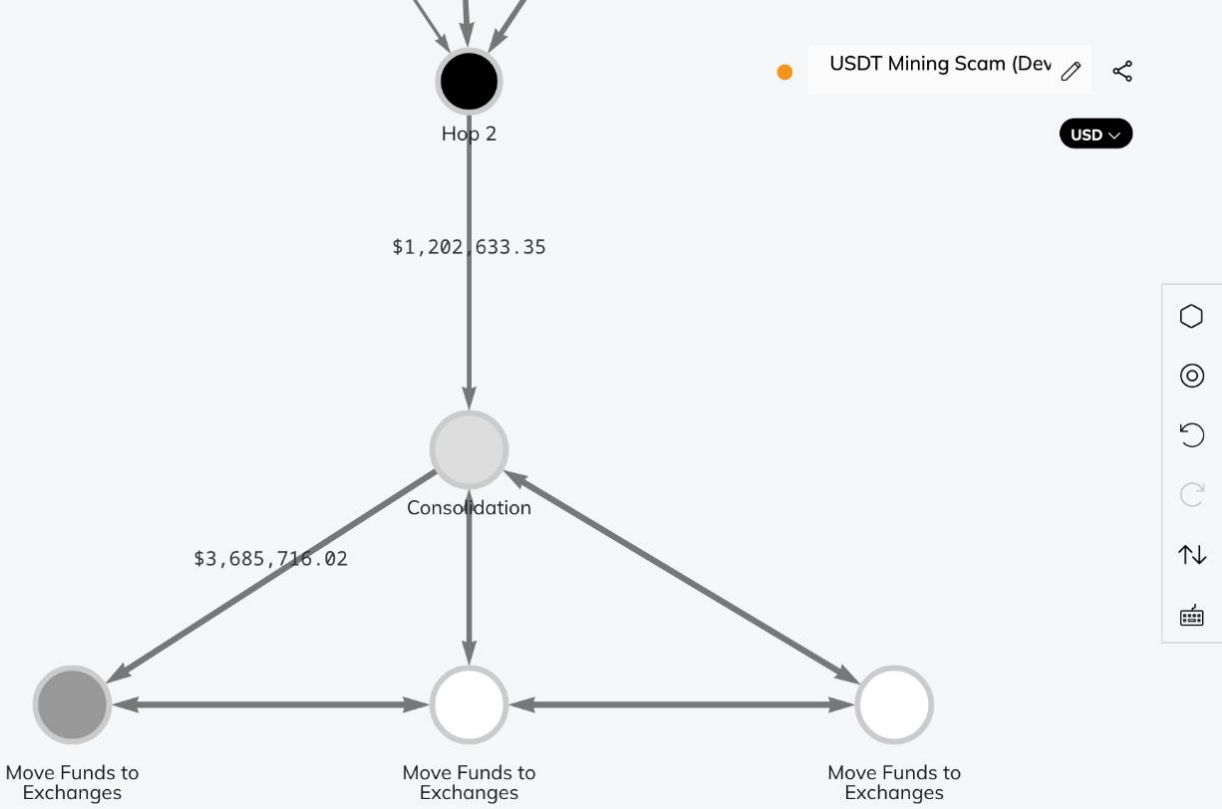
Initial Movements



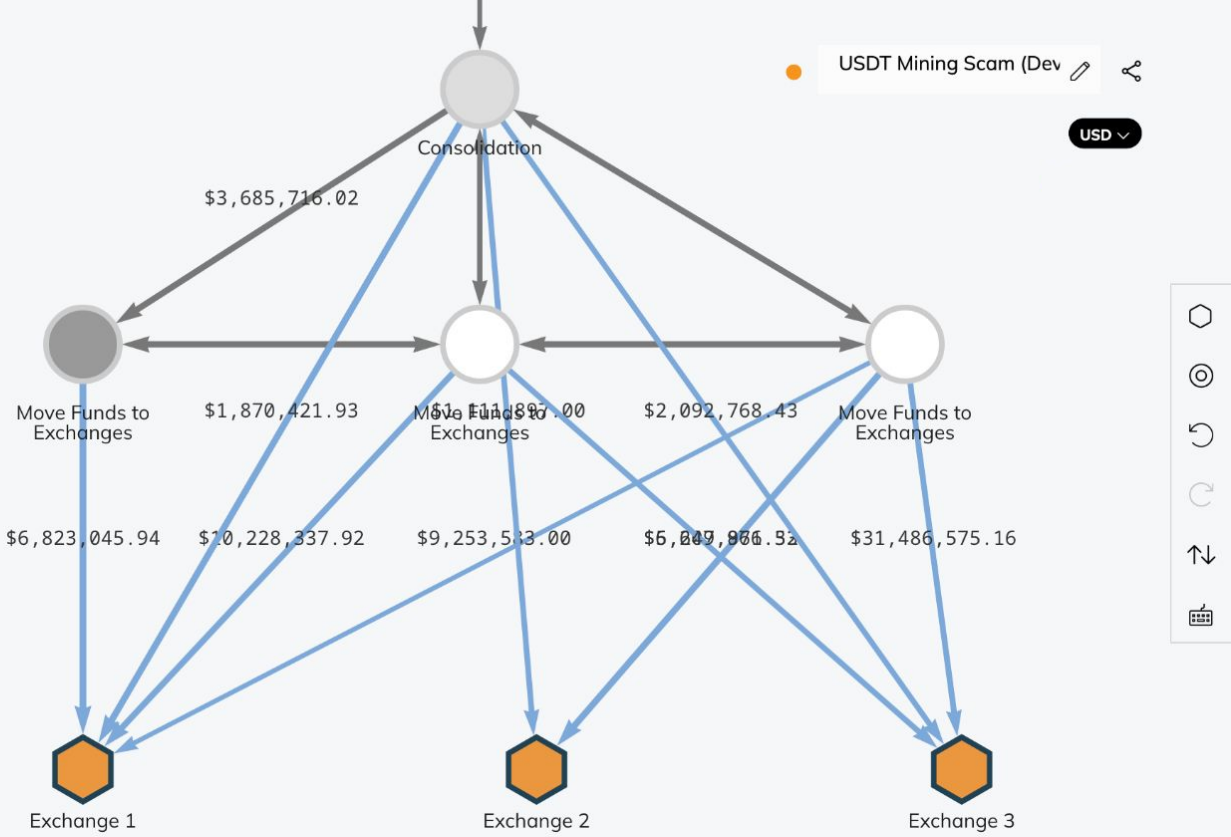
Consolidation



Movement to Exchanges



Deposits to Exchanges



$143M additional stolen value identified
($227M in total)

$1.2B
Value sent to cash-out points at exchanges

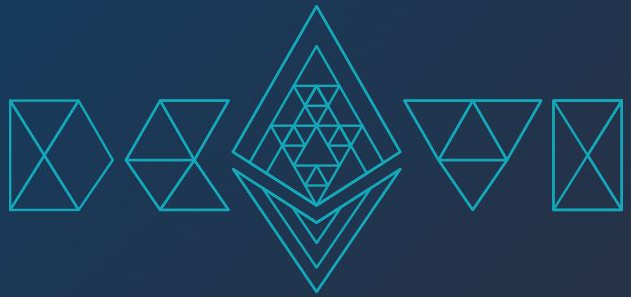
Identified repeated recipient addresses across scam approvers that indicate coordinated efforts

375 additional potential scam approvers

Section 4

Community Collaboration

How can we raise costs for bad actors?



Thank you!

Julia Hardy

Senior Investigator, Chainalysis

julia.hardy@chainalysis.com

@julia27eth

Adam Hart

Senior Training Specialist, Chainalysis

adam.hart@chainalysis.com

@Hart_Adam_