



**MERKLE SCIENCE**

**How criminals are using DeFi for illicit activity**

# Speaker Intro



- **Merkle Science** - Founding Team & Associate Director
- **Institute of Blockchain** - Vice President
- Qualified Advocate & Solicitor
- ISO TC307 committee
- Compliance Association & Network of Singapore
- Blockchain Association of Singapore - Regulatory Sub-Committee
- SFA Recognised Fintech Leader under 30 (2021)

# Decentralised Finance (DeFi) Risks



## Hack Track: Analysis of C.R.E.A.M. Finance Hack

C.R.E.A.M. Finance suffered yet another exploit this year, the attack stole over \$136 million worth of funds through flash loan attacks

News and Announcements Hack Track Merkle Science

5 minute read - November 9, 2021



## Hack Track: Analysis of the Bilaxy Hack

After the ERC-20 hot wallets hack, Bilaxy urges users to not deposit any funds into Bilaxy Accounts.

Blog Hack Track Merkle Science

4 minute read - September 1, 2021



## Hack Track: Initial Analysis of Liquid Global Security Breach

Hot wallets of Liquid were compromised in a security breach. Liquid has suspended all deposits and withdrawals in addition to moving digital assets to cold wallets. Read the blog to learn more

Blog Hack Track Merkle Science

2 minute read - August 19, 2021



## Hack Track: An Analysis of Poly Network Hack and Latest Related Events

On 10 August 2021, the Poly Network was attacked by a hacker, losing over \$600 million — the largest crypto hack since the Coincheck hack in 2018 — across the Ethereum, Binance Smart Chain, and Polygon blockchains. Read the blog to learn more

Blog Hack Track Merkle Science

5 minute read - August 12, 2021

- **Smart Contract Risk**
- **Governance Risk**
- **Oracle Risk**
- **Crypto Crime**

# **CASE STUDY 1**



# C.R.E.A.M HACK

In its THIRD exploit, the attackers found a vulnerability in the platform's lending system and exploited it to steal C.R.E.A.M. Finance's assets and tokens.

## Flash Loan

- ▶ From 0x961d2b694d909... To Curve.fi: y Swap For 0 iearn USDC (yUSDC)
- ▶ From 0x961d2b694d909... To Curve.fi: y Swap For 0 iearn USDT (yUSDT)
- ▶ From 0x961d2b694d909... To Curve.fi: y Swap For 0 iearn TUSD (yTUSD)
- ▶ From Black Hole: 0x000... To 0x961d2b694d909... For 447,202,022.713276945512955672 (\$505,338,285.67) Curve.fi yDA... (yDAI+y...)
- ▶ From Black Hole: 0x000... To 0x961d2b694d909... For 446,756,774.416766306389278551 Curve Y Pool... (yUSD)
- ▶ From 0x961d2b694d909... To 0x4b5bfd5212478... For 447,202,022.713276945512955672 (\$505,338,285.67) Curve.fi yDA... (yDAI+y...)
- ▶ From 0x961d2b694d909... To Cream.Finance: cr... For 446,756,774.416766306389278551 Curve Y Pool... (yUSD)
- ▶ From Cream.Finance: cr... To 0x961d2b694d909... For 22,337,774,341.38713187 Cream yUSD (crYUSD)
- ▶ From Aave: aWETH Tok... To 0xf701426b8126b... For 524,102.159298234706604104 (\$2,116,528,919.09) Wrapped Ethe... (WETH)
- ▶ From 0xf701426b8126b... To 0x961d2b694d909... For 6,000 (\$24,230,340.00) Wrapped Ethe... (WETH)

Scroll for more ↕



# C.R.E.A.M Exploit

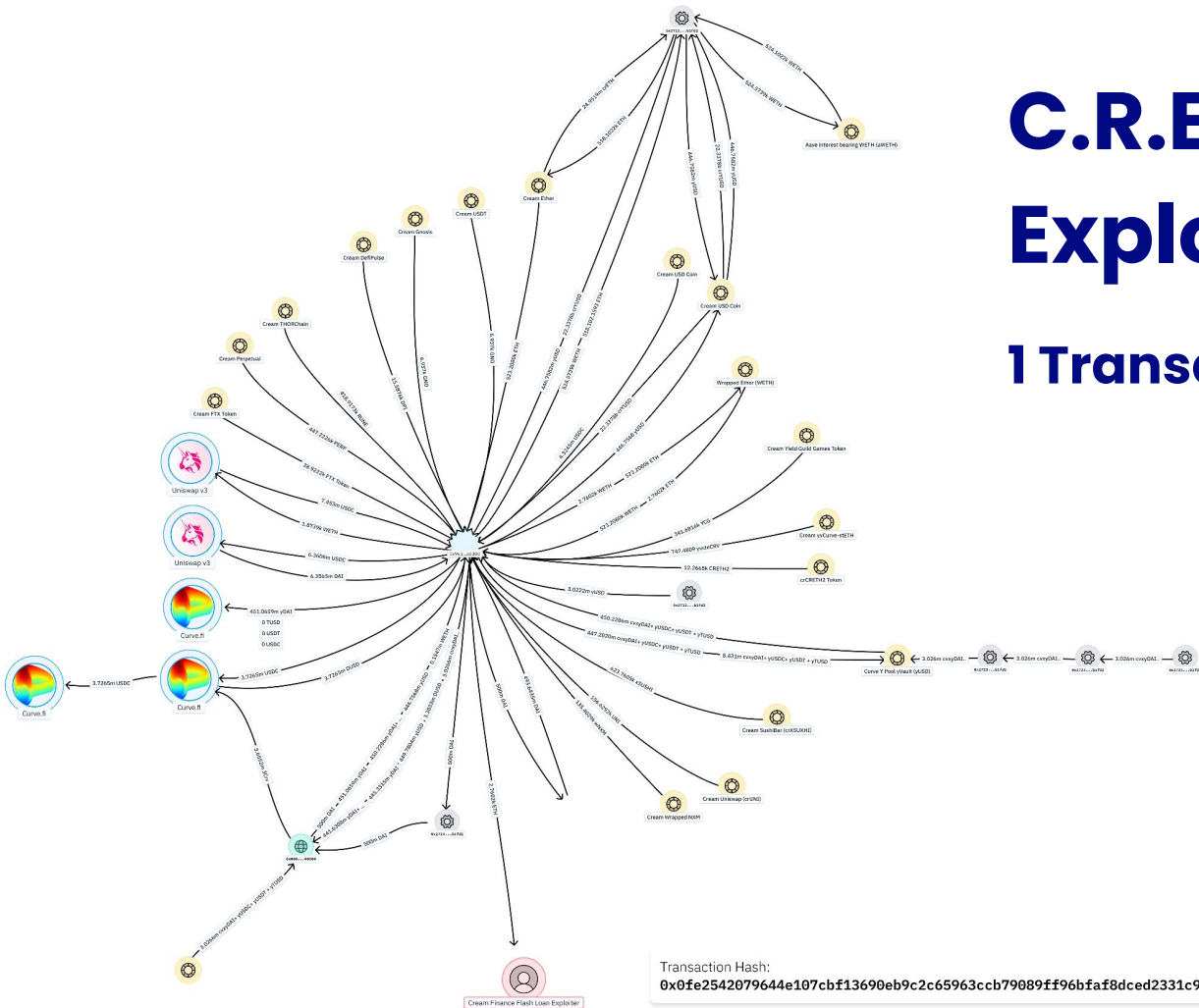
0 Transaction



Transaction Hash:  
`0x0fe2542079644e107cbf13690eb9c2c65963ccb79089ff96bfaf8dced2331c92`



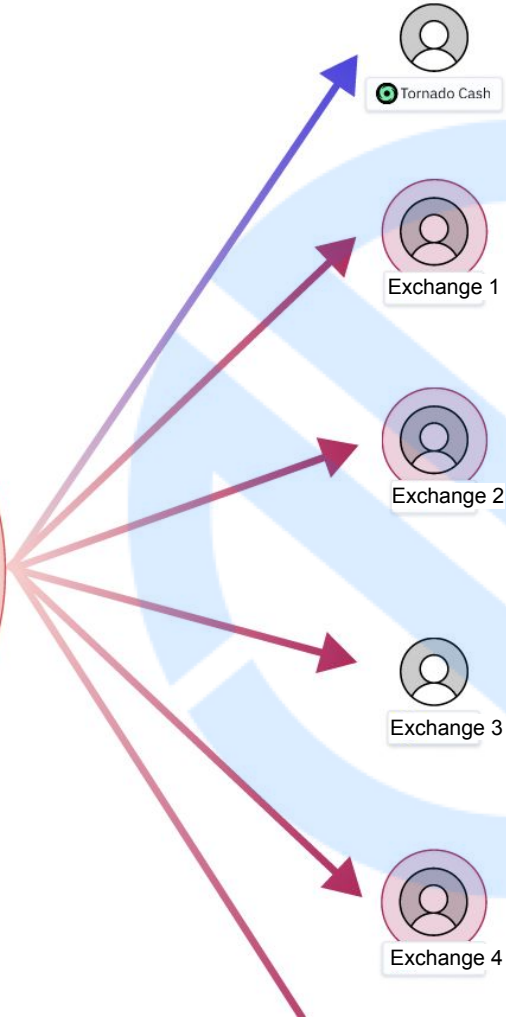
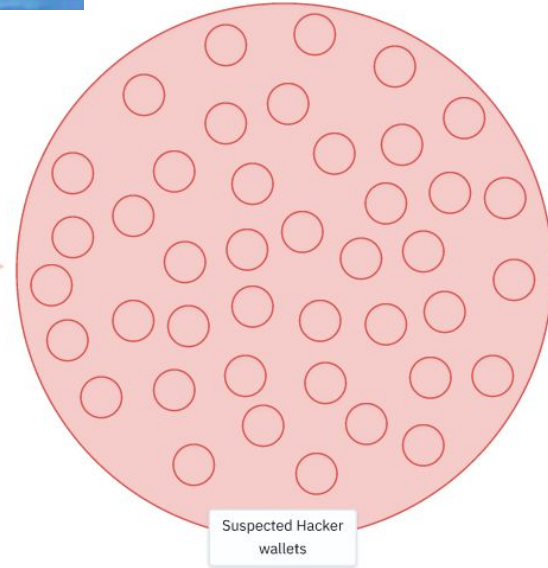
# C.R.E.A.M Exploit 1 Transaction



# **CASE STUDY 2**



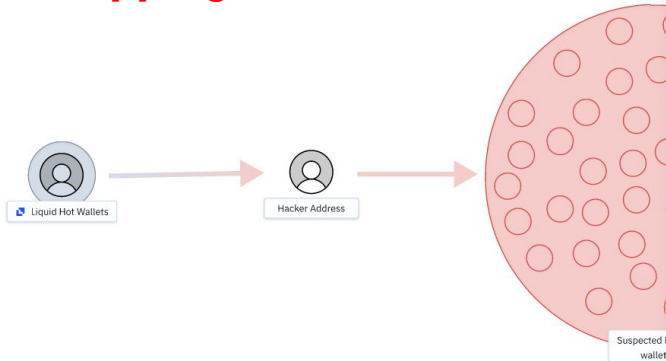




**On August 19th, Liquid detected unauthorized access of some of the crypto wallets managed at Liquid....**



69 different crypto assets were misappropriated and sent to other exchanges or **DeFi swapping venues**



Transaction Overview | Transaction Details

Etherum Transactions | **Token Transfers** | Internal Transactions

ERC-20

DAI	2,298.4036 DAI   \$2,298.40	0xab9317A3d1C141b...7294742EF3CD77A	Unknown	0xe82906b6B1B04f63...A57a3A7B6a99d9	Binance Exchange > Decentralised
UniFi	1,792.24398 UniFi	0x02D436DC483f445...37db0eE661949842	UniswapV3 Exchange > Decentralised	0x27239549DD40EA...C4196923745B1FD2	Unknown
WETH	0.7671538 WETH   \$2,409.10	0x27239549DD40E1D...C4196923745B1FD2	Unknown	0x02D436DC483f445...37db0eE661949842	UniswapV3 Exchange > Decentralised
UniFi	1,792.24393 UniFi	0x27239549DD40EA...C4196923745B1FD2	Unknown	0xab9317A3d1C141b...7294742EF3CD77A	Unknown

ERC-721

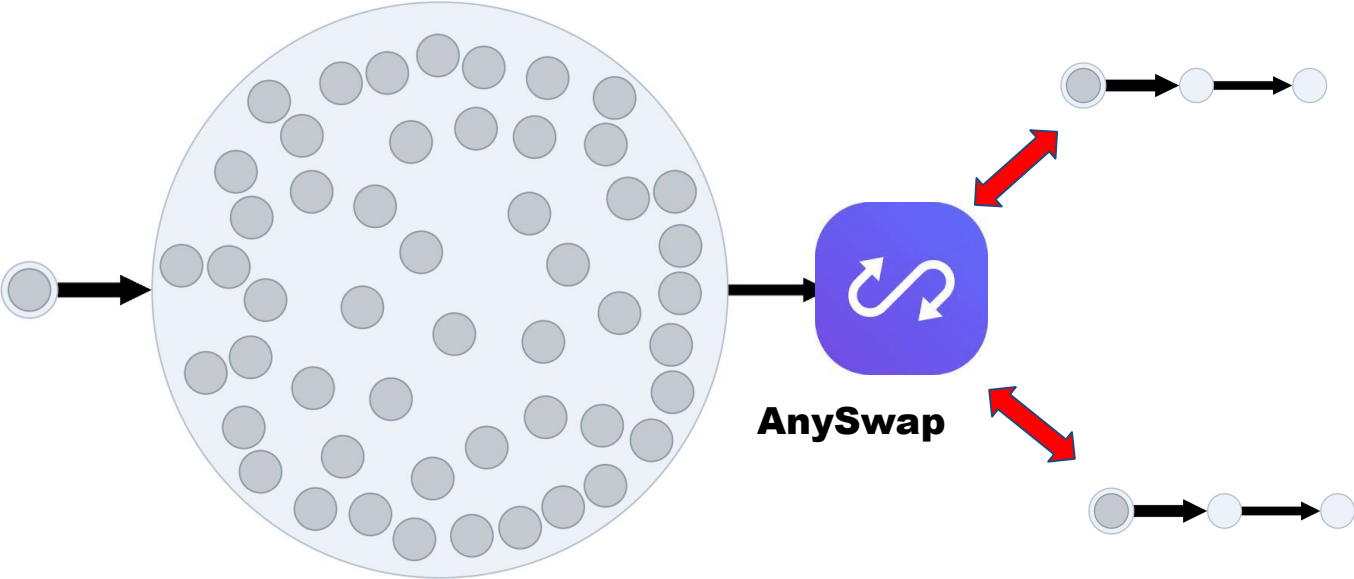
ERC-1155

# **CASE STUDY 3**



# CASE STUDY 3

# BONDLY Exploit



**Why is DeFi so popular for  
money laundering...**



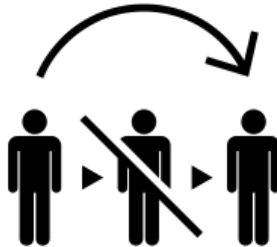
# Why is DeFi so popular for money laundering...

1. Criminals **retain control** of the asset
2. Ability to be accessed by anyone, anywhere, anytime.
  - Convenient and liquid for criminals to cash out
3. Automated Systems
  - All trades/swaps are done automatically and **irreversible**
  - Multiple transactions can all be executed at the same time



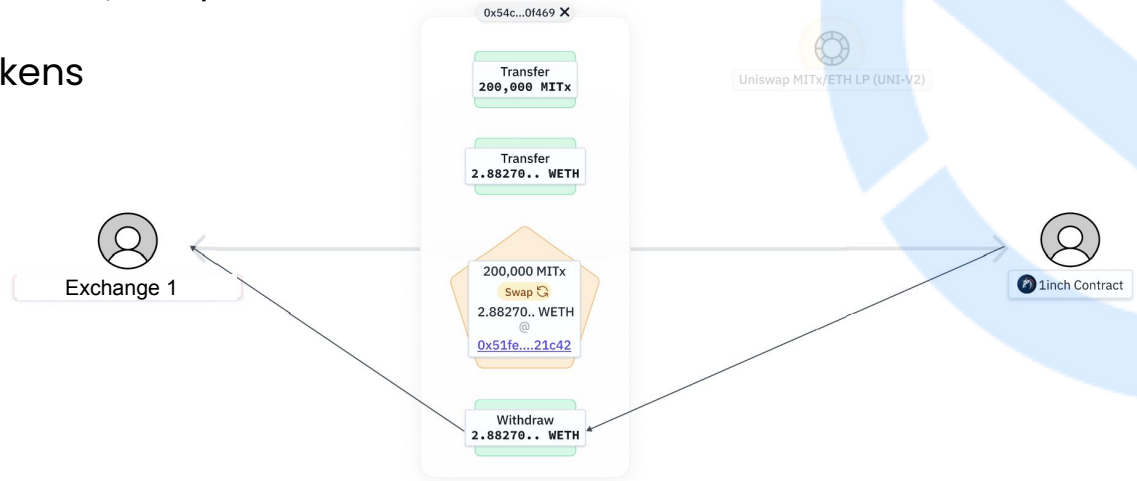
# Why is DeFi so popular for money laundering...

4. Regulations have not yet caught yet
5. Lack of Intermediaries
  - Automated systems means no one conducting KYC/AML checks (this will likely change over time)
6. Used to try and obfuscate source of funds from blockchain analytic firms



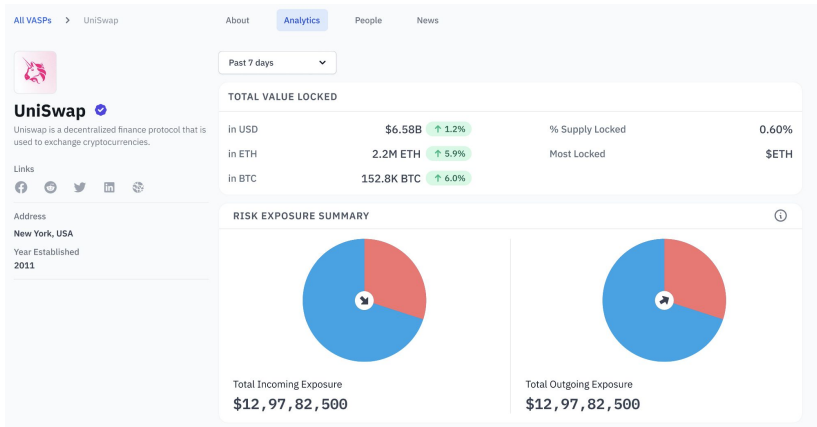
# Examples of how can DeFi can be used for money laundering...

1. Swaps;
2. Using stolen assets as collateral; and/or
3. Cross Chain - Wrapped tokens






# Evolution of DeFi



1. New Regulations by FATF
2. Increasingly number of DeFi platforms opting to implement KYC/AML
3. New solutions designed to monitor DeFi platforms and decipher smart contracts

Ouro aims to derive its innovations manifested in the growth of the value of crypto assets and migrates them onto OURO, making it an inflation-proof store of value.

[Research](#)

Requirement	KYC
Access	Everyone
Pay in	 IDIA

### Your Status

Open for KYC ?  
Contact [Synaps](#) for KYC support.

Verify KYC

No staked tokens in this pool.

Subscrip



You are connected to Binance Smart Chain



28 : 02 : 50 : 10  
DAYS HOURS MINS SECS

Subscribe to the Public Sale by staking IDIA token and reserve your allocation.

- This sale requires you to pass KYC. Your identity is tied to the connected wallet you use during KYC.
- You must hold at least 25 IF or 50 IDIA in your wallet to proceed with the KYC.
- You can only use a wallet that has passed KYC to subscribe, get allocation, purchase and claim.

Founded in 2018

**Merkle Science envisions a world powered by crypto.**

We are the catalysts enabling crypto companies — trailblazers and disruptors which are pushing the boundaries of innovation — to scale and mature so that a full range of individuals, entities, and services may transact with crypto safely.

CLIENTS & PARTNERS

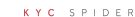
100/x



ASSOCIATIONS



ECOSYSTEM PARTNERS



LOCATIONS

London

Bangalore

Singapore

New York



# Thank You



[contact@merklescience.com](mailto:contact@merklescience.com)



[/Merkle-Science](https://www.linkedin.com/company/merkle-science)



[@merklescience](https://twitter.com/merklescience)



[/merklescience](https://www.facebook.com/merklescience)