

■ ■ ■ ■ ■
SECURITY BREACH: (//) EAST WING (//)

> SATELLITE CONNECTION ESTABLISHED
> RECEIVING DATA... 1%

> SATELLITE CONNECTION ESTABLISHED
> RECEIVING DATA... 1%

> INITIATE
PACQUET
PACQUET



CRYPTOCURRENCIES & FINANCIAL CRIME LAW ENFORCEMENT GUIDE

· GLOBAL PERSPECTIVES FROM EXPERTS ·

SECURITY BREACH [X] EAST WING [X]

> SATELLITE CONNECTION ESTABLISHED

> RECEIVING DATA... 1%

> SATELLITE CONNECTION ESTABLISHED

> RECEIVING DATA... 1%

< INITIATING >

< INITIATING >



CRYPTOCURRENCIES & FINANCIAL CRIME LAW ENFORCEMENT GUIDE

· GLOBAL PERSPECTIVES FROM EXPERTS ·



Dr. Jerry I. Akubo

Chief Executive Officer,
Technology Against Crime, Africa

Dr. Jerry Akubo founded TAC Africa as a futurist oriented, Law Enforcement Centric NGO, borne out of an International Forum on Technologies – a high level meeting dedicated to Technologies for a Safer World, co-organized by INTERPOL and the Ministry of Interior in Lyon, France in 2013. The NGO was officially registered in Abuja, Nigeria in 2016. Prior to this, he worked over a decade and half as the National Technical Officer for INTERPOL NCB Abuja under the auspices of the Nigeria Police Force.

Dr. Akubo has been recognized by the INTERPOL Global Complex for Innovation and the Directorate of Innovation Center, Singapore for his exemplary service, partnership and contributions having actively attended and participated in over eight (8) INTERPOL General Assemblies and Eight (8) INTERPOL World Congress in a roll amongst other high level technical meetings and presentation he organized on extending INTERPOL Secured Communications Network to authorized Law Enforcement Agencies across the African Region.

He is a frequent speaker on Emerging Technologies and the maximal utilization of INTERPOL tools by Law Enforcement Agencies within the African Region while pushing a number of research and developmental projects to improve the technical know-how and easy accessibility of tools and technologies for Law Enforcement Agents especially the front line officers.

Dr. Akubo is an evangelist on the use of Innovative Aerial Surveillance, remote sensing and emerging technology to tackle most unique set of challenges the African region is facing including on the one side. Transnational Organized Cyber Crime and on the other, battling insurgents and terrorist group often domiciled in very remote & inaccessible locations.

Table of Contents

**HOW CRIMINALS ARE USING
DEFI FOR ILLICIT ACTIVITY**

**WHY DEFI IS SO POPULAR
FOR MONEY LAUNDERING...**

**EXAMPLES OF HOW DEFI CAN
BE USED FOR MONEY LAUNDERING...**

EVOLUTION OF DEFI

**DECENTRALIZED FINANCE: CRIME DETECTION AND
PREVENTION IN DEFI**

**FRAUD INVESTIGATIONS WITH
ENHANCED BLOCKCHAIN ANALYSIS**

HOW CRIMINALS ARE USING DEFI FOR ILLICIT ACTIVITY

CASE STUDY

1

C.R.E.A.M HACK -

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

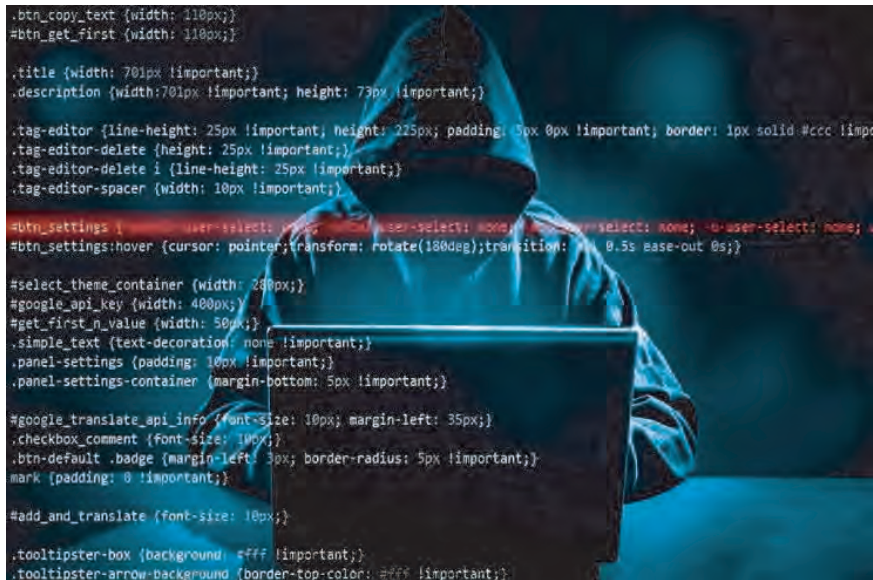
Flash Loan

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 yDAI... (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 yDAI... (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 Ether... (WETH)
From 0xf701426b8126b...	To 0x961d2b694d909...	For 6,000	(\$24,230,340.00) Wrapped Ether... (WETH)

Scroll for more ↗

C.R.E.A.M EXPLIOT

0 Transaction



```
.btn_copy_text {width: 110px;}
#btn_get_first {width: 110px;}

.title {width: 701px !important;}
.description {width: 701px !important; height: 73px !important;}

.tag-editor {line-height: 25px !important; height: 225px; padding: 5px 0px !important; border: 1px solid #ccc !important;}
.tag-editor-delete {height: 25px !important;}
.tag-editor-delete i {line-height: 25px !important;}
.tag-editor-spacer {width: 10px !important;}

#btn_settings {user-select: none; #user-select: none; #user-select: none; #user-select: none; #user-select: none;}
#btn_settings:hover {cursor: pointer; transform: rotate(180deg); transition: 0.5s ease-out 0s;}

#select_theme_container {width: 240px;}
#google_api_key {width: 400px;}
#get_first_n_value {width: 50px;}
.simple_text {text-decoration: none !important;}
.panel-settings {padding: 10px !important;}
.panel-settings-container {margin-bottom: 5px !important;}

#google_translate_api_info {font-size: 10px; margin-left: 35px;}
.checkbox_comment {font-size: 10px;}
.btn-default .badge {margin-left: 3px; border-radius: 5px !important;}
mark {padding: 0 !important;}

#add_and_translate {font-size: 10px;}

.tooltipster-box {background: #fff !important;}
.tooltipster-arrow-background {border-top-color: #fff !important;}
```

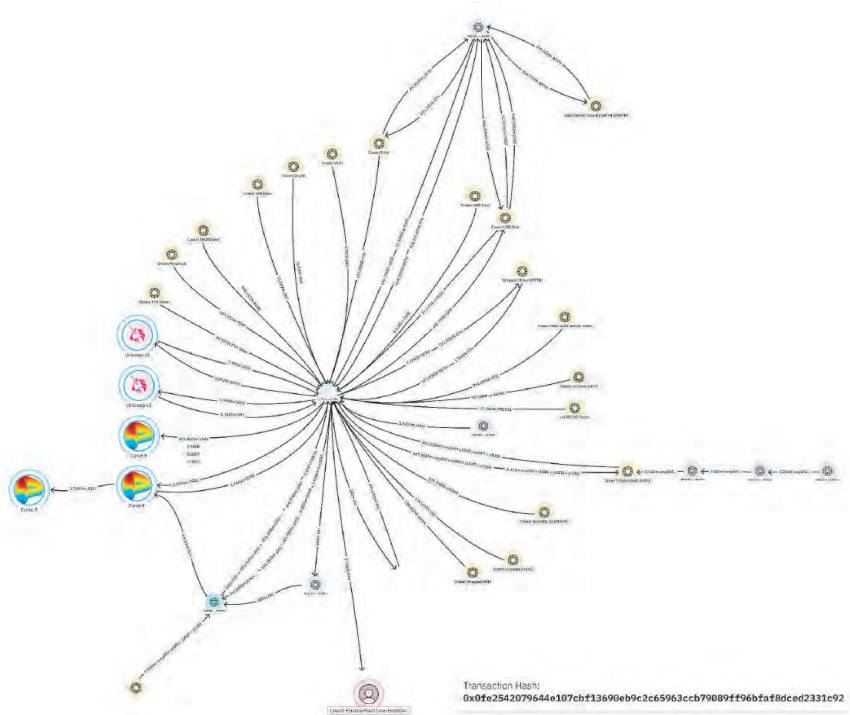
Cream Finance Flash Loan Exploiter

TRANSACTION HASH :

0x2446f1fd773fbb9f080e674b60c6a033c7ed7427b8b9413cf28a2a4a6da9b56c

C.R.E.A.M EXPLIOT

1 Transaction



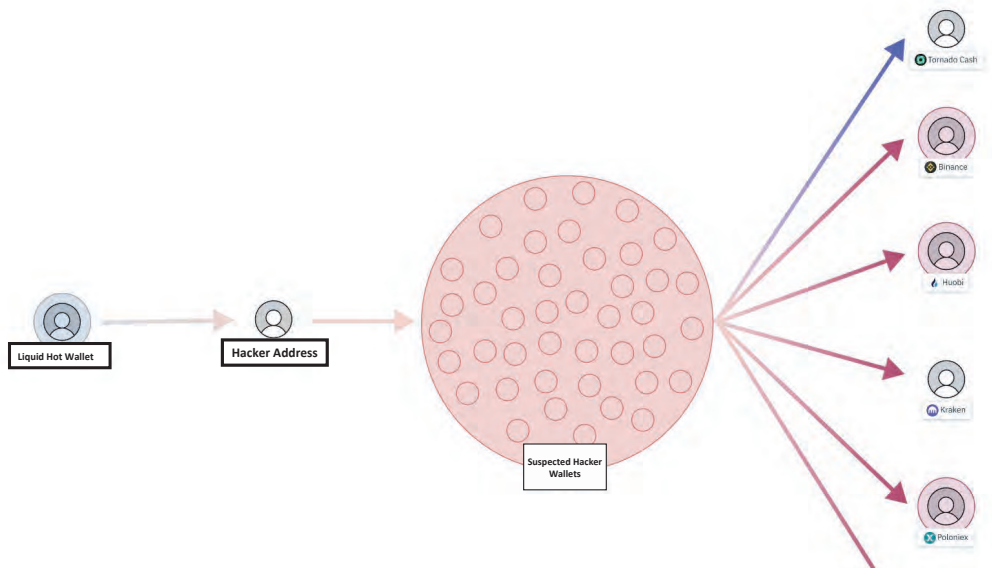
TRANSACTION HASH :

0x2446f1fd773fbb9f080e674b60c6a033c7ed7427b8b9413cf28a2a4a6da9b56c

CASE STUDY

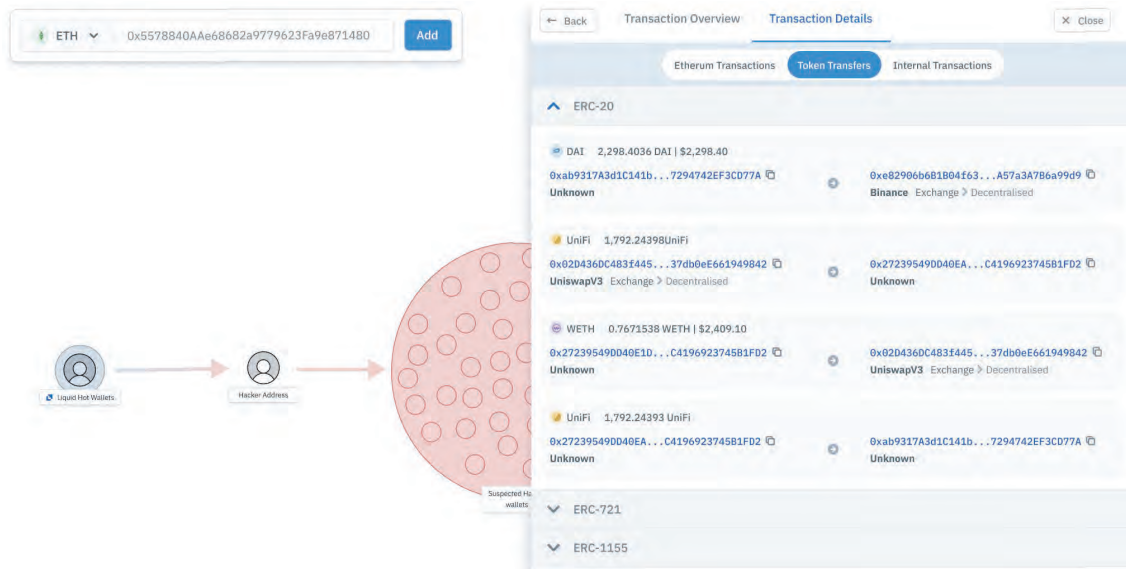
2

Attacker stole around \$91 Million in Cryptocurrency from liquid Global Hot Wallets



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

Attacker stole around \$91 Million in Cryptocurrency from liquid Global Hot Wallets

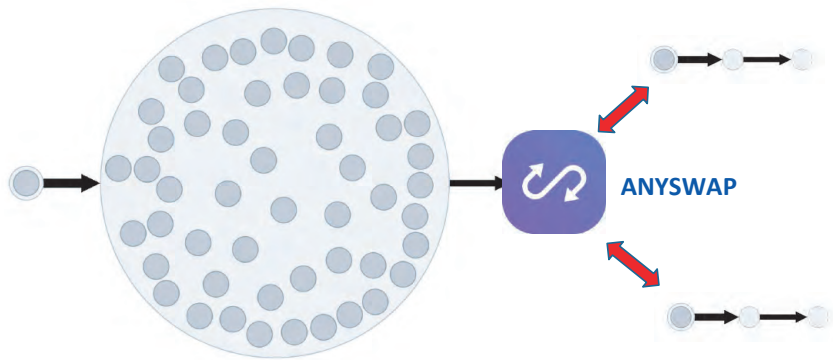


69 different crypto assets were misappropriated and sent to other exchanges or DeFi swapping venues

CASE STUDY

3

BONDLY EXPLIOT



WHY DEFI IS SO POPULAR

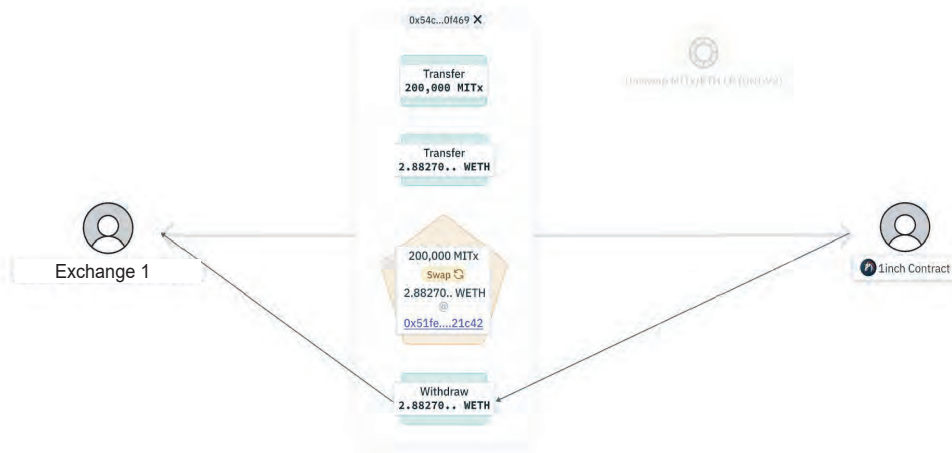
FOR MONEY LAUNDERING...

WHY IS DEFI SO POPULAR FOR MONEY LAUNDERING...

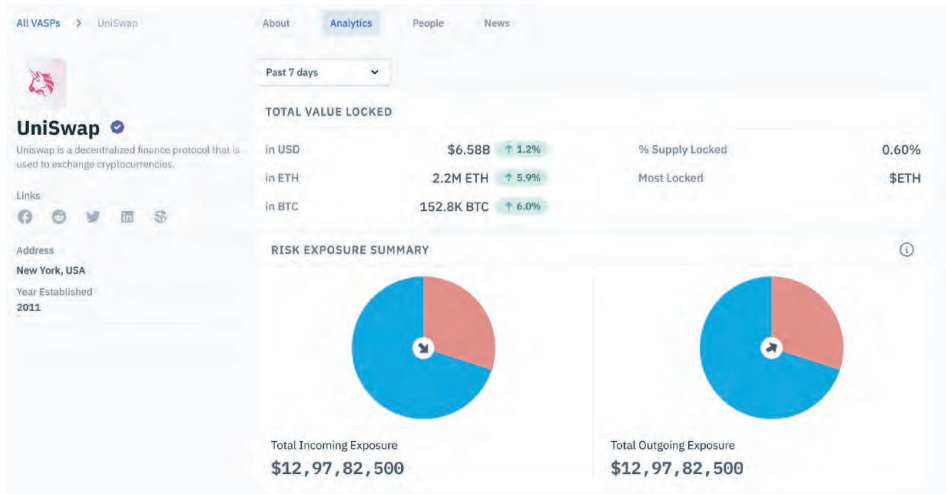
1. Criminals retain control
2. Ability to be accessed by anyone, anywhere, anytime.
 - Convenient and liquid for criminals to cash out easily
3. Automated Systems
 - All trades/swaps are done automatically and
 - Multiple transactions can all be executed at the same time
4. Regulations have not yet caught up yet
5. Lack of Intermediaries (likely change over time)
 - Automated systems means no one conducting KYC/AML
6. Used to try and obfuscate source of funds from blockchain analytic firms

EXAMPLES OF HOW 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

This example of
Single::ToString(),
Single::ToString(IFormatProvider), and
Single::ToString(String*, IFormatProvider)
generates the following output when run in the [en-US] c#
A Single number is formatted with various combinations
strings and IFormatProvider.

IFormatProvider is not used; the default culture is [en]
No format string:
'N5' format string:
'E' format string:
'E5' format string:

11876.54
11.87654e+03
1.187654e+04
1.187654e+04

A CultureInfo object for [en-US] is used for the [en]
No format string:
'N5' format string:
'E' format string:
'E5' format string:

11876.54
11.87654e+03
1.187654e+04
1.187654e+04

CHAPTER 2:

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

WHAT IS AML/CFT AND WHY IS IT SO IMPORTANT?

Money laundering and terrorist financing (ML/TF) harm society in a number of ways. Money laundering facilitates and perpetuates crime and supports criminals. Terrorist financing facilitates the commitment of atrocities at home and abroad.

Together, they undermine the trust of citizens in financial institutions, negatively affect market integrity and threaten the stability of the financial system. ML/TF cannot be fought in isolation. Governments, public authorities and the private sector all have a role to play. Since its inception, the EBA has been working to foster a common approach by national competent authorities and financial institutions across the single market to anti-money laundering and countering the financing of terrorism (AML/ CFT), and to equip them to apply this approach effectively.

A common approach is important, because financial crime respects no borders and a weakness in one area of the single market opens up the entire single market to abuse

The high-profile scandals of the last few years have shown that, collectively, we must strengthen Europe's AML/CFT defenses. This is why the European legislature gave the EBA new powers to lead, coordinate and monitor EU supervisors' fight against ML/TF. It also gave us a new objective, to prevent the use of the financial system for the purposes of money laundering and terrorist financing.

We will use all of our powers and functions to fulfil our AML/CFT objective. We will lead the development of EU-wide AML/CFT policies and standards within our mandate, monitor risks to the integrity of the single market and coordinate supervisory actions at Union level to ensure that financial institutions apply effective and robust AML/CFT controls wherever they operate in the single market. We aim to make a real difference in the fight against financial crime.

WHAT IS CHANGING IN THE APPROACH TO AML/CFT?

The EBA, with the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), has led the development of AML/CFT policy for competent authorities and financial institutions in the EU. A series of joint AML/CFT standards, guidelines and opinions has transformed the way competent authorities and financial institutions approach AML/CFT. In 2019, the European legislature consolidated the AML/CFT mandates of all three European supervisory authorities within the EBA. It also gave the EBA a clear legal duty to contribute to preventing the use of the financial system for the purposes of money laundering and terrorist financing (ML/TF) and to lead, coordinate and monitor the AML/CFT efforts of all EU financial services providers and competent authorities.

The law implementing these powers and this mandate came into effect on 1 January 2020.

Although important, these changes constitute an evolutionary, not revolutionary, step in the EU's approach to AML/CFT, which remains based on a minimum harmonization directive and an associated strong focus on national law and direct supervision of financial institutions by national competent authorities. This reduces the degree of convergence and consistency the EBA's work can achieve. To the extent that this is possible under the EU's continuing minimum harmonization framework, we will use our new powers to:

LEAD: the establishment of AML/CFT policy and support its effective implementation by competent authorities and financial institutions across the European Union with a view to fostering an effective risk-based approach to AML/CFT with consistent outcomes

COORDINATE: across the EU and beyond by fostering effective cooperation and information exchange between all relevant authorities in a way that supports the development of a common understanding of ML/TF risks, strengthens risk-based AML/CFT supervision, ensures that emerging risks are dealt with promptly across the single market and ensures effective oversight of cross border financial institutions.

MONITOR: the implementation of EU AML/CFT standards to identify vulnerabilities in competent authorities' approaches to AML/CFT supervision and to take steps to mitigate them before ML/TF risks materialize.

WHAT HAS THE E.B.A DONE UNTIL NOW ON AML/CFT?

The EBA, ESMA and EIOPA have since their inception been responsible for fostering the consistent and effective implementation, by national competent authorities, of the EU's AML/CFT legislation. Together, we have led the development of AML/CFT policy, supported its implementation and fostered cooperation between competent authorities across the single market.

POLICY DEVELOPMENT

The European Supervisory Authorities (ESAs) have led the development of EU AML/CFT policy for national competent authorities and financial institutions. Through joint guidelines, the ESAs introduced a common understanding of the risk-based approach to AML/CFT and how it should be applied by financial institutions and competent authorities, and complemented this through work on key, practical aspects of AML/CFT supervision and compliance where relevant.

For example, we published specific, hands-on opinions when we found that financial institutions were reluctant to onboard asylum seekers from high-risk jurisdictions for fear of regulatory censure, and in order to take the fear out of innovative solutions in the AML/CFT compliance context.

IMPLEMENTATION AND CONVERGENCE

The EBA has supported the implementation of policy products and standards to foster the development of comparable and joined-up approaches by competent authorities to AML/CFT supervision, and to achieve consistent and effective outcomes in the implementation of the risk-based approach to AML/CFT.

We supported implementation through training and by identifying, assessing and disseminating information on EU-wide ML/TF risks, notably through the Joint Opinion on ML/TF risks, which we publish every 2 years. We also organized seminars to enhance competent authorities' understanding of ML/TF risks in specific sectors that are associated with higher ML/TF risk, including electronic money and money remittance.

More recently, we provided direct support to competent authorities in the context of our multi-annual, staff-led reviews of competent authorities' approaches to the AML/CFT supervision of banks. Where we found serious shortcomings in competent authorities' approaches to the AML/CFT supervision of financial institutions, we carried out enquiries and, in some cases, opened formal investigations and where necessary issued recommendations, notably where we found a competent authority was in breach of Union law.

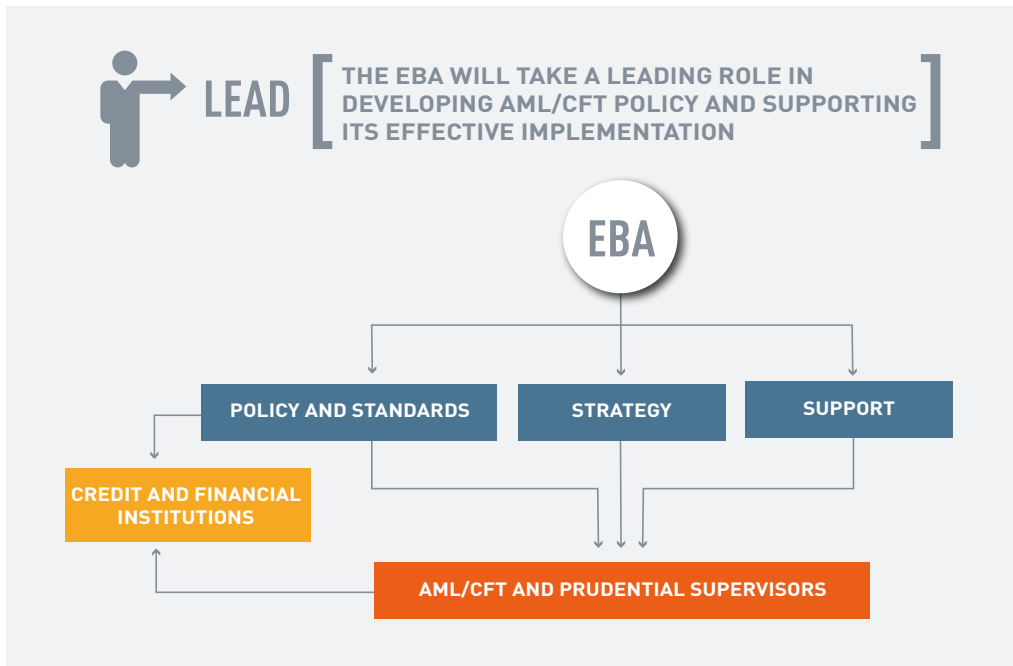
COOPERATION

Over the last 2 years, we have worked to raise awareness, for example in our 2018 report on prudential supervisory colleges, which lists examples of good practice, and in our 2019 opinion on the consideration of ML/TF risks in the prudential context. We also developed specific tools to foster effective cooperation between competent authorities.

These tools include an agreement that sets out the practical modalities for cooperation and information exchange between the European Central Bank in its capacity as prudential supervisor and all national AML/CFT supervisors, and, most recently, own-initiative guidelines on supervisory cooperation in the AML/CFT space.

These guidelines establish a framework for cooperation of competent authorities that includes the setting up of AML/CFT colleges, a new concept that has already been identified as good practice by international standard setters and mirrors the work that we have done in ensuring prudential colleges of supervisors work well. A new mandate for 2020 In 2019, the European legislature consolidated the AML/CFT mandates of all three ESAs within the EBA. It also gave the EBA a clear legal duty to contribute to preventing the use of the financial system for the purposes of ML/TF and to lead, coordinate and monitor the AML/CFT efforts of all EU financial services providers and competent authorities. The law implementing these powers and mandate came into effect on 1 January 2020. This means that the EBA is from now on solely responsible for leading, coordinating and monitoring AML/CFT efforts across the entire EU financial sector.

How will the EBA 'lead' on AML/CFT?



“OUR OBJECTIVE IS TO TAKE A LEADING ROLE IN DEVELOPING AML/CFT POLICY AND IMPLEMENTATION”

A person is seen from the side, working on a laptop. The image is heavily overlaid with a dark blue, semi-transparent filter. The person's hair is dark and slightly messy. The laptop screen shows some graphical elements, but they are not clearly visible due to the overlay. The overall mood is technical and focused.

CHAPTER 3:

DECENTRALIZED FINANCE: CRIME DETECTION AND PREVENTION IN DEFI

DECENTRALIZED FINANCE

CORE PRINCIPLES

Decentralized finance leverages key principles of the Ethereum blockchain to increase financial security and transparency, unlock liquidity and growth opportunities, and support an integrated and standardized economic system.

Programmability. Highly programmable smart contracts automate execution and enable the creation of new financial instruments and digital assets.

IMMUTABILITY: Tamper-proof data coordination across a blockchain's decentralized architecture increases security and auditability.

INTEROPERABILITY: Ethereum's composable software stack ensures that DeFi protocols and applications are built to integrate and complement one another. With DeFi, developers and product teams have the flexibility to build on top of existing protocols, customize interfaces, and integrate third-party applications. For this reason, people often call DeFi protocols "money legos."

TRANSPARENCY: On the public Ethereum blockchain, every transaction is broadcast to and verified by other users on the network (note: Ethereum addresses are encrypted keys that are pseudo-anonymous). This level of transparency around transaction data not only allows for rich data analysis but also ensures that network activity is available to any user. Ethereum and the DeFi protocols running on it are also built with open source code that is available for anyone to view, audit, and build upon.

Permissionless: Unlike traditional finance, DeFi is defined by its open, permissionless access: anyone with a crypto wallet and an Internet connection, regardless of their geography and often without any minimum amount of funds required, can access DeFi applications built on Ethereum.

SELF-CUSTODY: By using Web3 wallets like MetaMask to interact with permissionless financial applications and protocols, DeFi market participants always keep custody of their assets and control of their personal data.

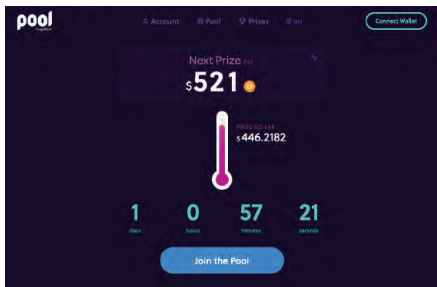
WHAT ARE THE USE CASES FOR DECENTRALIZED FINANCE

From DAOs to synthetic assets, decentralized finance protocols have unlocked a world of new economic activity and opportunity for users across the globe. The comprehensive list of use cases below is proof that DeFi is much more than an emerging ecosystem of projects. Rather, it's a wholesale and integrated effort to build a parallel financial system on Ethereum that rivals centralized services because it is profoundly more accessible, resilient, and transparent.

Data and Analytics

Because of their unprecedented transparency around transaction data and network activity, DeFi protocols offer unique advantages for data discovery, analysis, and decision-making around financial opportunities and risk management. The explosive growth of new DeFi applications has spurred the development of numerous tools and dashboards, such as *DeFi Pulse*, that help users track the value locked in DeFi protocols, assess platform risk, and compare yield and liquidity.

Gaming

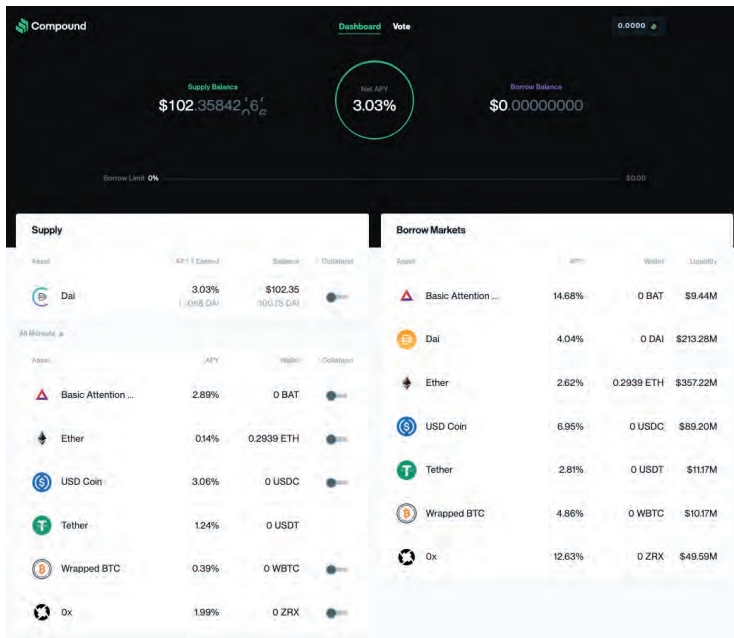


PoolTogether is a no-loss, audited savings game powered by Ethereum.

The composability of DeFi has unlocked opportunities for product developers to build DeFi protocols directly into platforms across a variety of verticals. Ethereum-based games have become a popular use case for decentralized finance because of their built-in economies and innovative incentive models. PoolTogether, for example, is a no-loss audited savings lottery that enables users to purchase digital tickets by depositing the DAI stablecoin, which is then pooled together and lent to the Compound money market protocol to earn interest.

Lending & Borrowing

Peer-to-peer lending and borrowing protocols are some of the most widely used applications in the DeFi ecosystem. Compound, for example, is an algorithmic, autonomous interest rate protocol that integrates with and underlies a long list of DeFi platforms, including PoolTogether, Argent, and Dharma. By providing interest rate markets on Ethereum, Compound allows users to earn interest on crypto that they've supplied to the lending pool. The Compound smart contract automatically matches borrowers and lenders and calculates interest rate based on the ratio of borrowed to supplied assets. Compound is a compelling example of the exponential opportunity of the DeFi space: as more products integrate the Compound protocol, more and more crypto assets will be able to earn interest, even when idle.



Compound is an algorithmic, autonomous interest rate protocol.

Staking

As the Ethereum network transitions to a Proof of Stake consensus algorithm with Ethereum 2.0, users will have the opportunity to stake their ETH and earn rewards, either as validators or through staking providers. Staking on Eth2 is analogous to an interest-bearing savings account: stakers receive interest (rewards) for validating blocks on the Ethereum protocol.

Synthetic Assets

Related to stablecoins, synthetic assets are crypto assets that provide exposure to other assets such as gold, fiat currencies, and cryptocurrencies. They are collateralized by tokens locked into Ethereum-based smart contracts, with built-in agreements and incentive mechanisms. The Synthetix protocol, for example, implements a 750% collateralization ratio, which helps the network absorb price shocks.

Tokenization

Tokenization is one of the cornerstones of decentralized finance and a native functionality of the Ethereum blockchain. Tokens not only fuel the network but also unlock a variety of economic possibilities. Simply speaking, a token is a digital asset that is created, issued, and managed on a blockchain. Tokens are designed to be secure and instantly transferable, and they can be programmed with a range of built-in functionalities.

IS STABLECOIN THE ANSWER TO ALL CRYPTOCURRENCY PROBLEMS?

What Are Stablecoins?

Whether it's the U.S. dollar or Dogecoin, a currency is most useful as a medium of exchange and a store of value. Price stability is crucial to those functions. For that reason, policymakers aim to keep the price of traditional national currencies broadly stable. In forex trading of fiat currencies, a 2% move in a day is a landslide.

How Stablecoins Maintain Valuations

some stablecoins seek to tame volatility by pegging their price to the U.S. dollar, and by backing the value of their tokens with liquid reserves of collateral. Stablecoins can be divided into three groups based on how they choose to pursue price stability.

Fiat-collateralized stablecoins: The value of these stablecoins is backed by fiat currency like the U.S. dollar. Collateral can also consist of precious metals like gold and silver and commodities like crude oil. Collateral must be held by a custodian and audited regularly to guarantee redemption of the stablecoin tokens. Tether and TrueUSD are popular stablecoins pegged at par to the U.S. dollar and are backed by dollar reserves.²³

Crypto-collateralized stablecoins: Crypto-collateralized stablecoins are similar to those backed by fiat, except that their underlying collateral is another cryptocurrency or basket of cryptocurrencies instead of a fiat currency or a commodity.

Algorithmic stablecoins: Whether collateralized or not, algorithmic stablecoins rely on an algorithm, or a set of rules, to control the supply of tokens, thereby keeping the value stable.

For example, an algorithmic stablecoin may rely on a rule that requires changes in token supply sufficient to maintain the stablecoin's value. This is somewhat akin to a central bank's role in increasing or decreasing interest rates to ensure stable prices. The difference is that central banks like the U.S. Federal Reserve set monetary policy based on widely understood parameters and back that policy with an unlimited supply of legal tender. Algorithmic stablecoins like Basis and TerraUSD lack such advantages.

Drawing The Line

The increasing adoption of stablecoins could help popularize the use of cryptocurrencies as a medium of exchange for routine financial transactions, as well as for other applications. Whether it's the U.S. dollar or Dogecoin, a currency is most useful as a medium of exchange and a store of value. Price stability is crucial to those functions. For that reason, policymakers aim to keep the price of traditional national currencies broadly stable. In forex trading of fiat currencies, a 2% move in a day is a landslide.

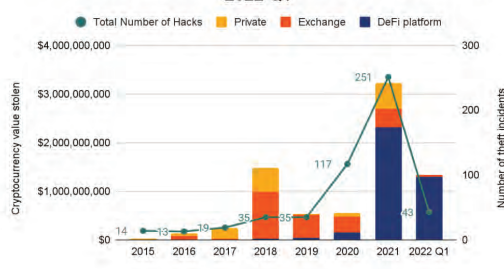
Such applications may include using stablecoins to trade goods and services over blockchain networks, in decentralized insurance solutions, derivatives contracts, financial applications like consumer loans, and prediction markets.

DEFI HACKS ON THE RISE

(As seen on Chainalysis)

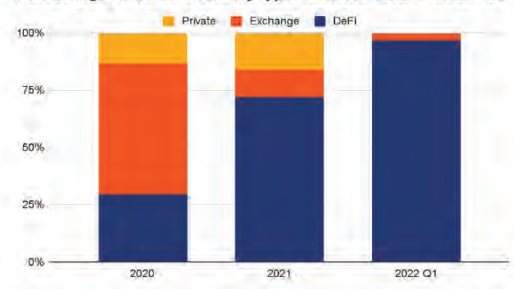
Digital thieves had a big year in 2021, stealing \$3.2 billion worth of cryptocurrency. But in 2022, they're shaping up to steal even more. In the first three months of this year, hackers have stolen \$1.3 billion from exchanges, platforms, and private entities—and the victims are disproportionately in DeFi.

Total number of thefts and value stolen by type of victim, 2015 - 2022 Q1



Almost 97% of all cryptocurrency stolen in the first three months of 2022 has been taken from DeFi protocols, up from 72% in 2021 and just 30% in 2020.

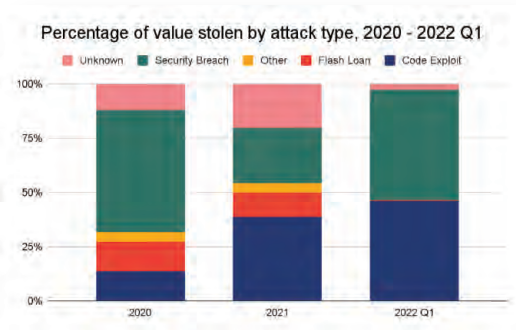
Percentage of value stolen by type of victim, 2020 - 2022 Q1



Code exploits are an increasingly common vector of attack, but security breaches are here to stay

In the past, cryptocurrency hacks were largely the result of security breaches in which hackers gained access to victims' private keys—the crypto-equivalent of pickpocketing. Ronin Network's March 2022 breach, which enabled the theft of \$615 million in cryptocurrency, has proven the continued effectiveness of this technique.

Chainalysis aggregate data further illustrates this fact. From 2020 to Q1 2022, 35% of all cryptocurrency value was stolen thanks to a security breach.



Note: The "unknown" label means information about hack type is not publicly available. The "other" label means the hack type is known but does not fit within our defined categories.

Digital thieves had a big year in 2021, stealing \$3.2 billion worth of cryptocurrency. But in 2022, they're shaping up to steal even more. In the first three months of this year, hackers have stolen \$1.3 billion from exchanges, platforms, and private entities—and the victims are disproportionately in DeFi.

Code exploits occur for a number of reasons. For one, in keeping with DeFi's faith in decentralization and transparency, open-source development is a staple of DeFi applications. This is an important and generally positive trend: since DeFi protocols move funds without human intervention, users should be able to audit the underlying code in order to trust the protocol. But this benefits cybercriminals, too, who can analyze the scripts for vulnerabilities and plan exploits well in advance.

In the DeFi hack of BadgerDAO last year, for example, the hacker tested the exploit and laundering process months before the attack.

FOLLOWING THE MONEY:

THE FINAL DESTINATION

How do hackers launder stolen cryptocurrency? In 2021, more stolen funds flowed to DeFi platforms (51%) and risky services (25%) than ever before. Centralized exchanges, formerly a top destination for stolen funds, fell out of favor, receiving less than 15% of the total. This is likely due to exchanges' embrace of AML and KYC processes, which threaten the anonymity of cybercriminals.

We've created a new category this year to reflect what may be a first in DeFi hacks we've observed: returns. In August of last year, the thief behind the \$600 million dollar Poly Network hack returned all \$613 million of the funds they stole, and refused the bug bounty they were offered.

In February 2022, U.S. authorities arrested two individuals who allegedly helped launder the funds taken from Bitfinex during the hack and were able to recover the majority of the total stolen. This is a very positive development for cryptocurrency users, but it remains to be seen whether this seizure will prompt hackers to change their money laundering strategies moving forward.

As the total value locked in DeFi climbs to ever-greater all-time highs — \$256 billion at last peak — so too does the risk of exploitation. If there's one takeaway from the meteoric rise in thefts from DeFi platforms, it's the need for smart contract security and price oracle accuracy. Code audits, decentralized oracle providers, and an altogether more rigorous approach to platform security could be the ideal means to that end.

Fortunately, even when these functions do fail and cryptocurrencies are stolen, blockchain analysis can help. Investigators with a full picture of the movement of funds from address to address can take advantage of opportunities to freeze or even seize assets in transit, stopping bad actors before they cash out.

This example of
Single::ToString(),
Single::ToString(String*),
Single::ToString(IFormatProvider*), and
Single::ToString(String*, IFormatProvider*)
generates the following output when run in the [en-US] c#
A Single number is formatted with various combinations
of strings and IFormatProvider.

IFormatProvider is not used; the default culture is [en]
No format string:
'N5' format string:
'E' format string:
'E5' format string:

11876.54
11.87654e+03
1.187654e+04
1.187654e+04

A CultureInfo object for [en-US] is used for the [en]
No format string:
'N5' format string:
'E' format string:
'E5' format string:

11876.54
11.87654e+03
1.187654e+04
1.187654e+04

CHAPTER 4:

FRAUD INVESTIGATIONS WITH ENHANCED BLOCKCHAIN ANALYSIS

To realize their full potential, cryptocurrencies unquestionably require high levels of trust and transparency. Blockchain analysis can help with the investigation, classification and monitoring of blockchain addresses and transactions so that investigators can comprehend the operations of various blockchain participants. Cryptocurrency transactions are handled using blockchain technology. As a result, it is prone to fraudulent acts, just like any other currency exchange platform. Blockchain analysis aids in the detection of fraud and suspicious activity.

For instance, when two rogue FBI agents stole Bitcoin (BTC) while investigating the Silk Road darknet market in 2015, a blockchain analysis platform called Chainalysis made headlines. Chainalysis is a blockchain data platform based on blockchain technology that helps government and business sectors detect and prevent the illegal use of cryptocurrencies.

Experienced criminals or sometimes qualified crypto investors frequently try to outsmart forensics organizations or crypto monitoring tools by employing a variety of techniques and strategies to restrict blockchain analysis.

For instance, using mixers is one of the most prevalent tricks that aggregate many senders' inputs while masking their addresses. All other addresses are untraceable because the mixed input is delivered from a single address, thus hiding the original sender. A mixer (also known as a tumbler) is a service that combines multiple streams of possibly traceable crypto assets. This enhances transaction anonymity by making crypto transactions more difficult to track.

In one investigation looking at bitcoin transfers to an illegal group, tracing efforts revealed a multitude of suspect transactions that went through a U.S.-based cryptocurrency exchange. Taking a closer look at the characteristics of these transactions, investigators tracked the origination accounts and found specific wallets that were indeed transferring money to the group's account. Additional clues in the transactions — such as dramatic variations in amounts — provided pivot points in the investigation to identify additional outputs to the same or other illicit entities. This gave adequate evidence to subpoena the exchange for the identity of the owners of the wallets in question and demand holds on their funds.

After tracing millions of transactions, executing hundreds of subpoenas and gathering donor information from exchanges, authorities were able to take action. Ultimately, the investigation resulted in a halt to funding, as well as the tracing of nearly every individual or party that donated to the group. Many of the donors traced had operated on U.S.-based exchanges and therefore could be personally identified and pursued. Moreover, the government now has a window to continue monitoring activity and ensure that no further transactions are completed.

While cryptocurrency is likely to remain under the microscope as a boon for criminal activity, robust and committed cryptocurrency tracing operations can actually be used to bring criminal parties to light. As the above example shows, in some ways, cryptocurrency is making it easier to account for the movement of terrorist and malicious parties and prevent finances from falling into the wrong hands.

Business looking to tap into the cryptocurrency and blockchain space can take a few steps to remain above board and conduct business in a transparent way. These include adhering to all regulations and guidance that exist, such as know your customer, anti-money-laundering and SEC parameters for tokens, and consulting with experts to verify that the proper protocols and processes are in place. It's also critical to test new products and programs extensively for security, functionality and compliance.

00000000

SECURITY BREACH: [/] EAST WING [/]

> SATELLITE CONNECTION ESTABLISHED

> RECEIVING DATA... 1%

> SATELLITE CONNECTION ESTABLISHED

> RECEIVING DATA... 1%

> INITIATE MISSILE

> ACQUISITION SUCCEEDED

> SECURITY BREACH

WWW.TACAFRICA.ORG

