INSIDER.

Jeudi 01 Juin 2023

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

CREOGN

CENTRE DE RECHERCHE DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

CAMPUS
CYBER

CAMPUS CYBER

COMMONS STUDIO.

- + EXPLORE
- + PRODUCE
- + SHARE

Explore complex subjects.
Identify and anticipate future market developments in cybersecurity.
Explore through risk reduction via mutualization.

Implement exploratory projects.
With the goal of producing deliverables: prototyping, proof of concepts.

Generate leverage effects for and by the ecosystem through the sharing of common resources.
Spread the perspectives and directions of the French ecosystem. Encourage the development of standards.
Enhance interoperability of French solutions.

THE STUDIO IN NUMBERS.

+ **20 Commons**

Products already produced or currently in production.

+ **14 Working Groups**

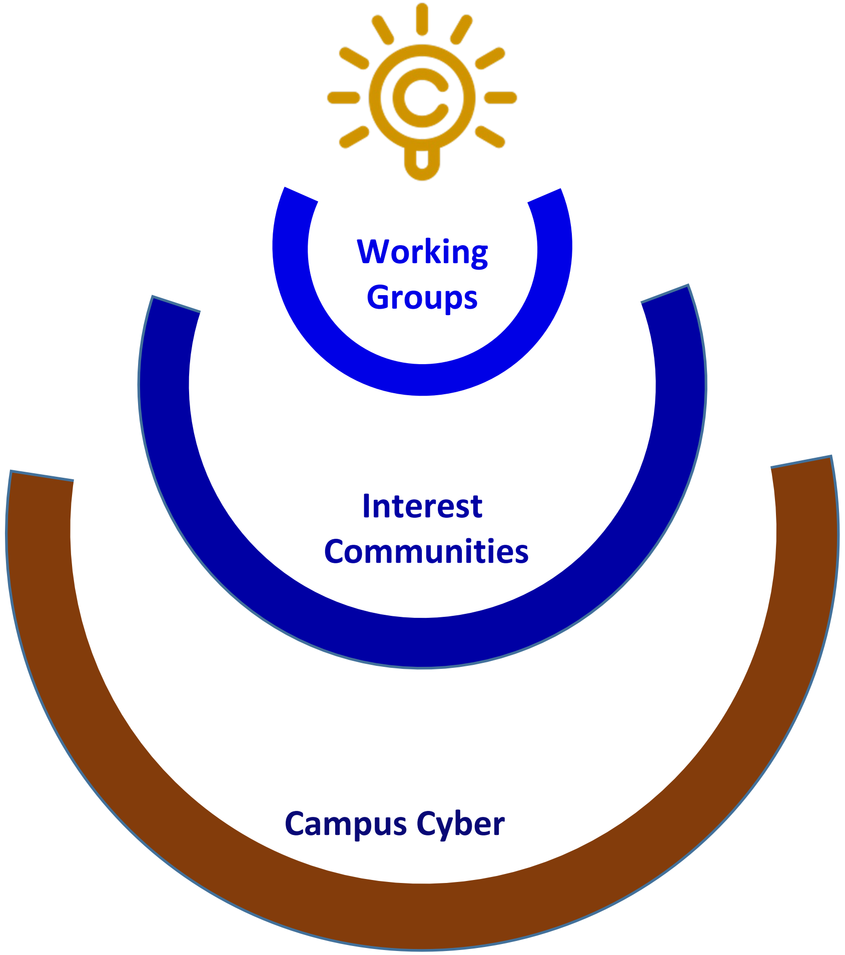
In total, including 12 ongoing ones, with approximately 10 groups consisting of 3 to 8 people.

+ **650 Individuals in the CI**

Places for exchange and definition of working groups.

+ **200 Organizations**

The entire ecosystem is involved in the work of the commons.



SPEAKERS

Christophe PELFRESNE
Banque de France
christophe.pelfresne@banque-france.fr

Stephan COHEN
BNP Paribas
stephan.cohen@bnpparibas.com

Karolina GORNA
LEDGER
karolina.gorna@ledger.fr

Jean-Loïc MUGNIER
EXPERT CYBERSECURITE WEB3
jeanloicmugnier@proton.me

Thomas BENOIT
SET IN STONE
thomas.benoit@setinstone.io

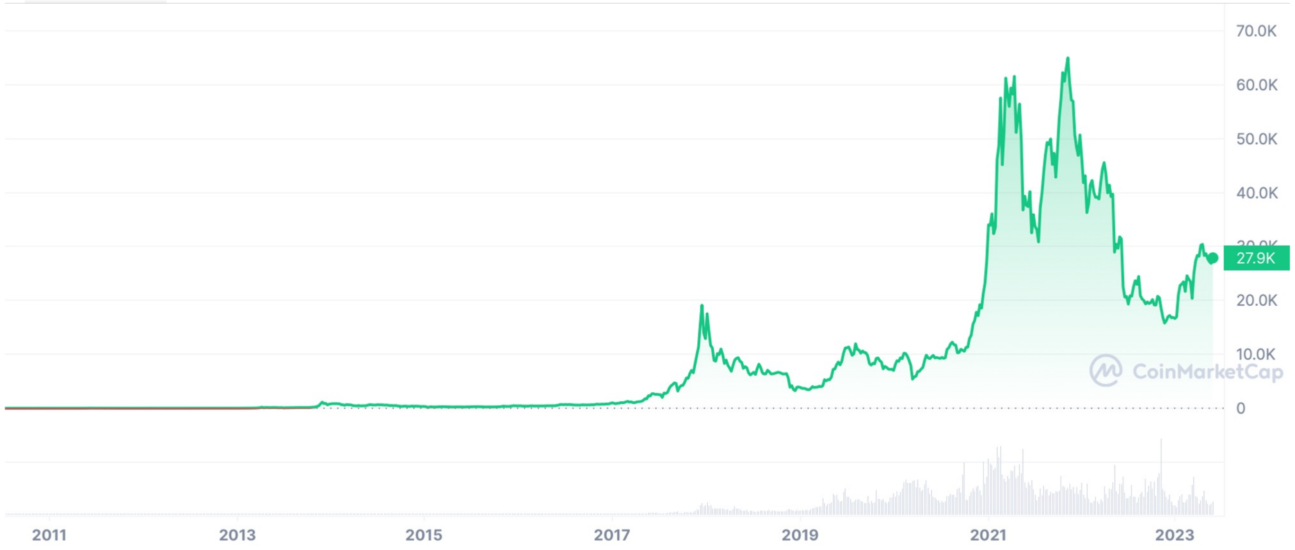
GT CRYPTO-ACTIF

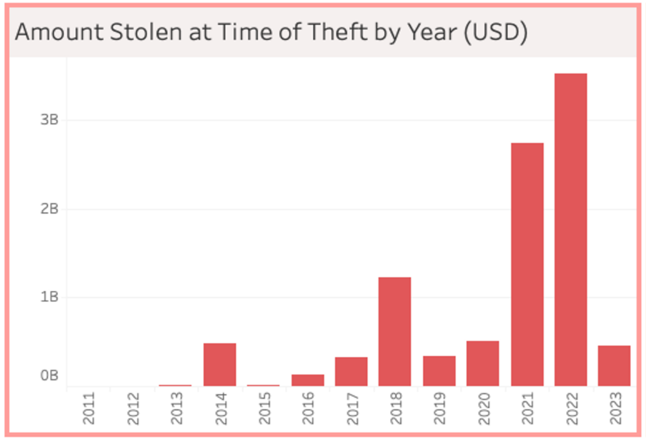
With the increasing interest in crypto assets such as Crypto coins and NFTs and it disruptive capabilities in several industries, we created a working group to dedicate our efforts on the study of the security of its underlying technologies: The distributed ledger technologies.

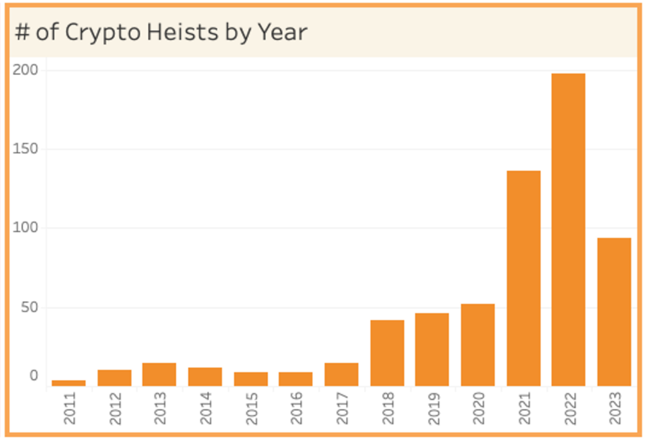
Among different studies, the group focused on the elaboration of a Catalog of Attacks emphasizing on:

- The Historic of known attacks
- The list of known vulnerabilites
- The Categorisation of the different type of attacks.

As time goes by, more and more attacks





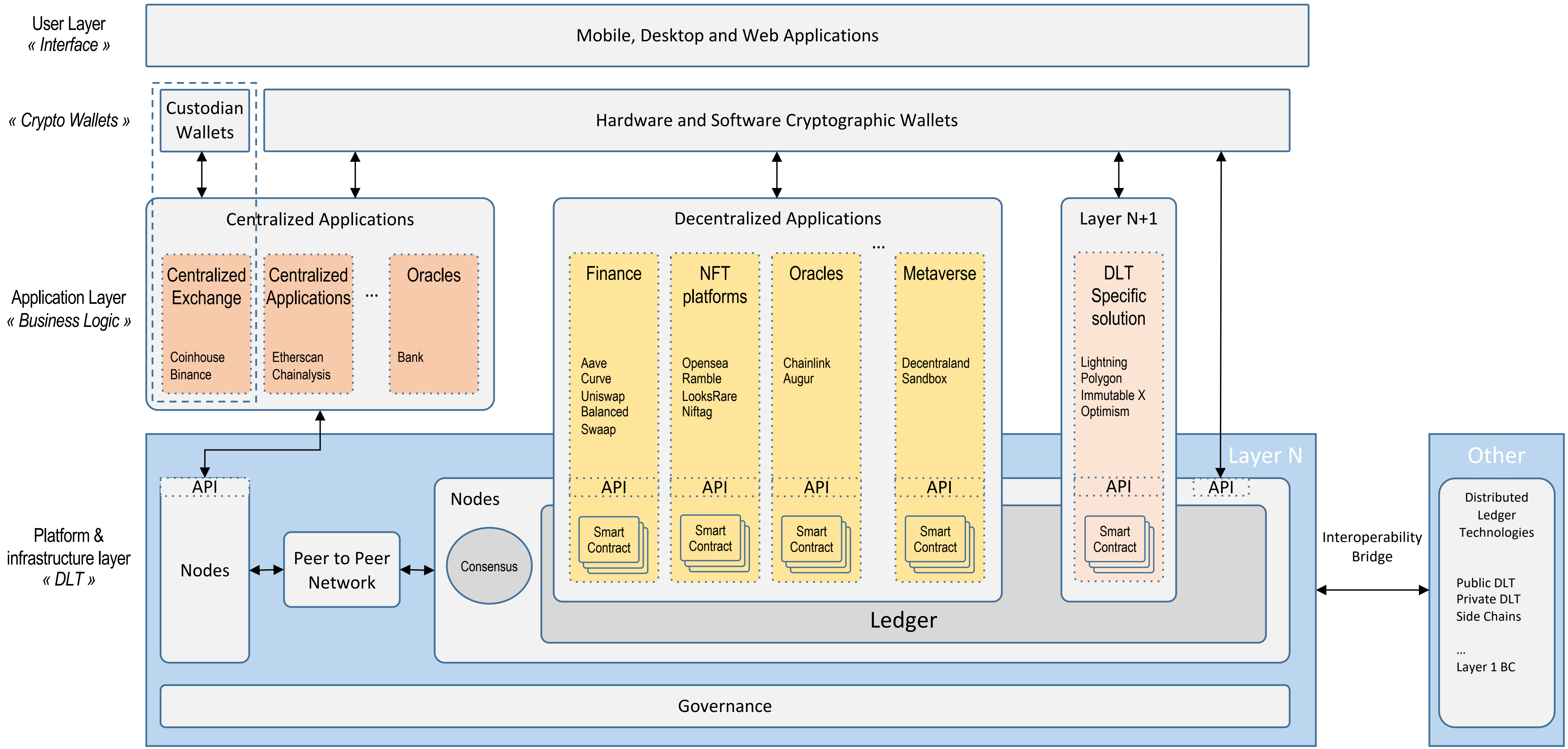


- **Timeline**
  As with cyber attacks, attacks on blockchain has known a continuous acceleration

- **Stolen amount**
  Although Bitcoin prices has fluctuated since the main heist have been recorded (from 2014), the amount stolen keeps getting higher and higher, with an acceleration since 2020

- **Attacks targets**
  Exchanges were the main target of attacks but a shift is in progress towards Defi

GLOBAL ARCHITECTURE



User Layer
« Interface »

Mobile, Desktop and Web Applications

« Crypto Wallets »

Custodian Wallets

Hardware and Software Cryptographic Wallets

Application Layer
« Business Logic »

Centralized Applications

- Centralized Exchange: Coinhouse, Binance
- Centralized Applications: Etherscan, Chainalysis
- …
- Oracles: Bank

Decentralized Applications

- Finance: Aave, Curve, Uniswap, Balanced, Swaap — API — Smart Contract
- NFT platforms: Opensea, Ramble, LooksRare, Niftag — API — Smart Contract
- Oracles: Chainlink, Augur — API — Smart Contract
- …
- Metaverse: Decentraland, Sandbox — API — Smart Contract

Layer N+1

- DLT Specific solution: Lightning, Polygon, Immutable X, Optimism — API — Smart Contract

Platform & infrastructure layer
« DLT »

Layer N

API

Nodes

Peer to Peer Network

Nodes

Consensus

Ledger

API

Governance

Interoperability Bridge

Other

Distributed Ledger Technologies

Public DLT
Private DLT
Side Chains
…
Layer 1 BC

COMPONENTS ATTACKS

USER INTERFACE

VULNERABILITIES

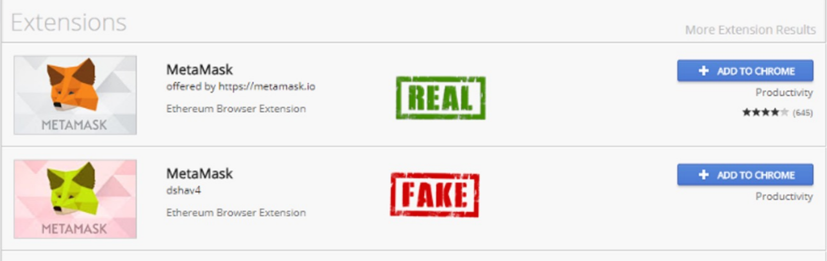
- Lack of awareness of risks and attacks (ex : phishing, fake sites)
- Lack of control over downloaded apps (ex : fake mobile apps)
- Lack of control for browser extensions (ex : fake extensions)
- Blind signing
- Misuse of security functions (ex : sim swap)
- Users credulity (ex : investment scam)
- Bad investor behavior (ex : rug pull, high profile doubler scam)
- Attacks targeting users

IMPACTS

- Revealing sensitive data such as wallet password, private key or seed phrase
- Stolen assets

Bored Ape Stolen via Phishing attack

PERFORMER	Unknown	**ANNÉE**	2022
VICTIM	Seth Green	**PAYS**	NA
IMPACT	Stolen NFT		
DESCRIPTION	The American director Seth Green had his Bored Ape NFT stolen in mid-May via a phishing link. It consists of pretending to be a known entity to extract confidential information from the Internet user: identifiers, connection codes, personal data. This technique had already been used at the end of April to steal “Bored Apes” NFTs from several crypto-collectors, for damage caused to several million dollars. The director, who had the intellectual property on the Bored Ape image, had to give up on the animated film project in which the monkey played the main role		


Extensions

More Extension Results

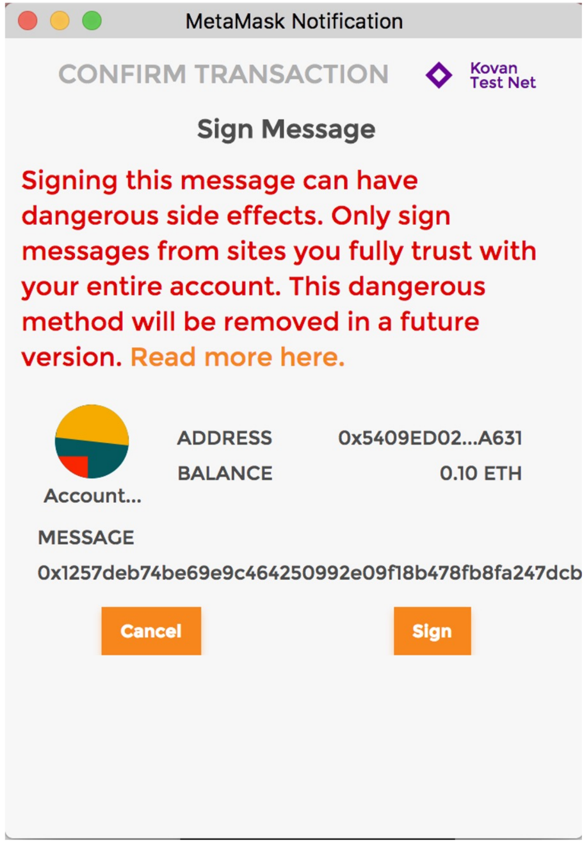
MetaMask
offered by https://metamask.io
Ethereum Browser Extension

MetaMask
dshav4
Ethereum Browser Extension

COMPONENTS ATTACKS

USER INTERFACE

Bored Ape Stolen via Phishing attack


MetaMask Notification

CONFIRM TRANSACTION

Kovan Test Net

Sign Message

Signing this message can have dangerous side effects. Only sign messages from sites you fully trust with your entire account. This dangerous method will be removed in a future version. Read more here.

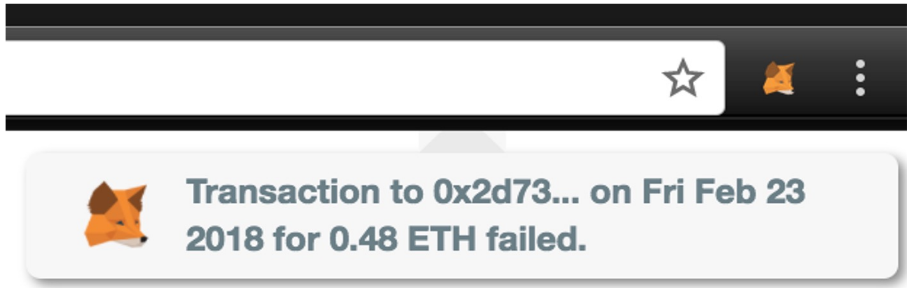
Account...

ADDRESS 0x5409ED02...A631

BALANCE 0.10 ETH

MESSAGE

0x1257deb74be69e9c464250992e09f18b478fb8fa247dcb


Transaction to 0x2d73... on Fri Feb 23 2018 for 0.48 ETH failed.

If Metamask wallet is unlocked in your browser

- Any websites is able to see your account address
- Create a fake notification about an **existing** transaction that supposedly failed.
- Trick you into signing a new transaction.
- When they are actually stealing your assets from your wallet.

Exploits

Data Layer (Smart contracts)

VULNERABILITIES

- A vulnerable implementation of smart contract logic.
- Lack of access control.
- Flaws in the programming language execution and toolchain.

IMPACTS

- Non-authorized code execution.
- Deny of service (Availability).
- Elevation of privileges.
- Financial losses.

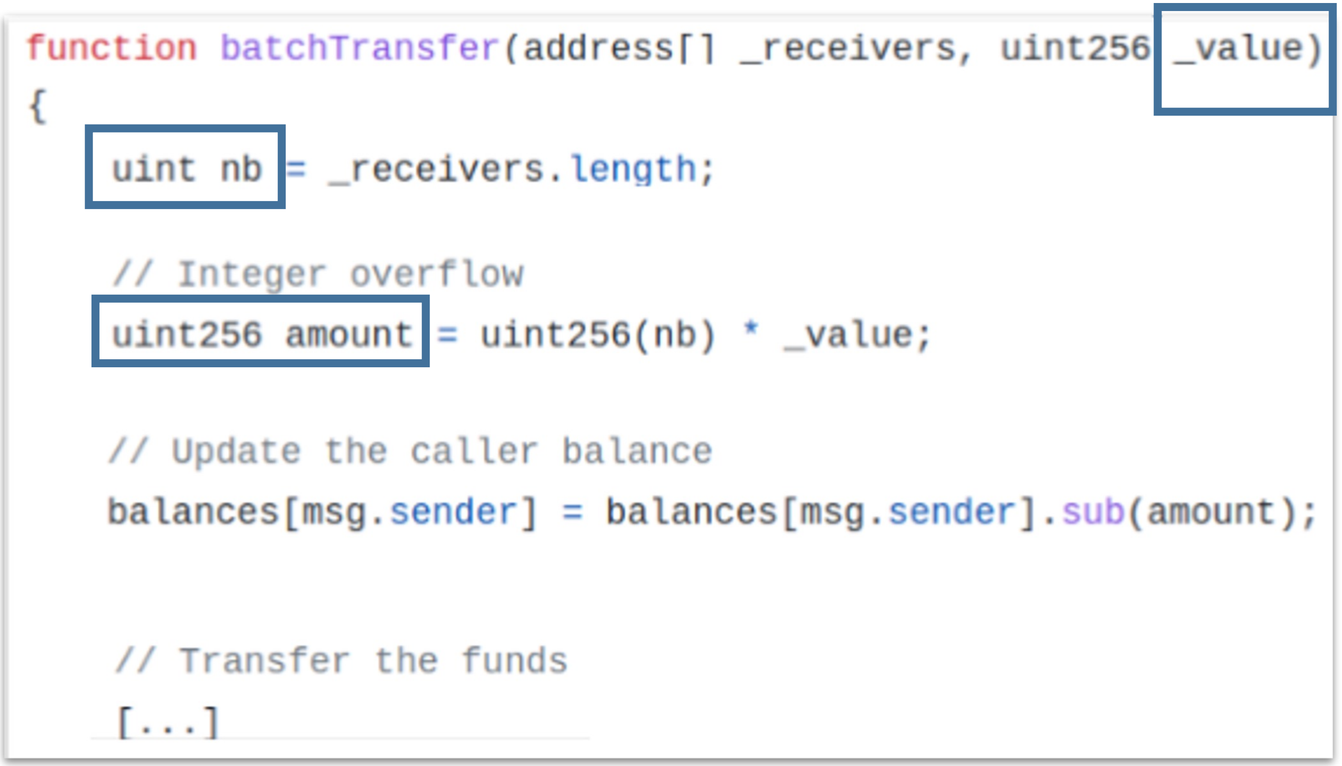
Attack on the Beauty Chain BEC token

PERFORMER	Unknown	**Year**	2018
VICTIM	Beauty Chain	**Country**	N/A
IMPACT	Attacker obtained 10^58 tokens for free		
DESCRIPTION	BEC token was the token used for the Beauty Chain project. As most utility tokens, they are defined by a set of few standardized smart contracts. In this case, The team implemented a non-standardized batch transfer function with a very simple vulnerability: an integer overflow. Using a specific set of parameters for this function would allow the attacker to obtain a huge amount of tokens out of thin air.		

Exploits

Data Layer Example

Attack on the Beauty Chain BEC token

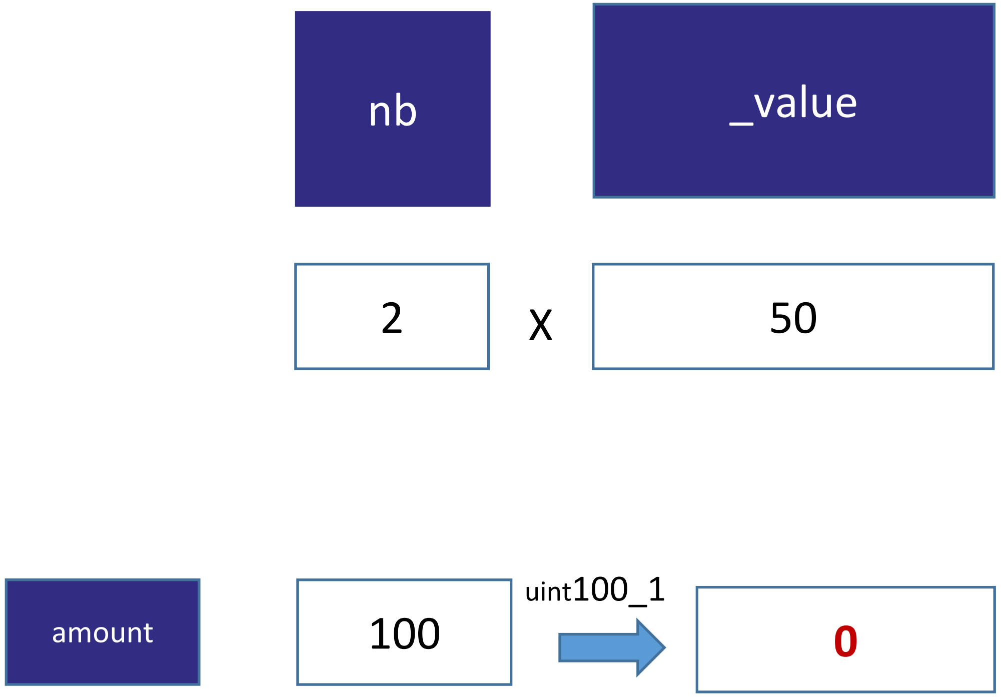


```
function batchTransfer(address[] _receivers, uint256 _value)
{
    uint nb = _receivers.length;

    // Integer overflow
    uint256 amount = uint256(nb) * _value;

    // Update the caller balance
    balances[msg.sender] = balances[msg.sender].sub(amount);


    // Transfer the funds
    [...]
```



$\text{uint100\_1} = \{0, 1, \ldots, 99\}$

Exploits

Decentralised Applications

VULNERABILITIES

- Price manipulations
- Vulnerable cross smart contract interactions
- Smart contracts misconfiguration.

IMPACTS

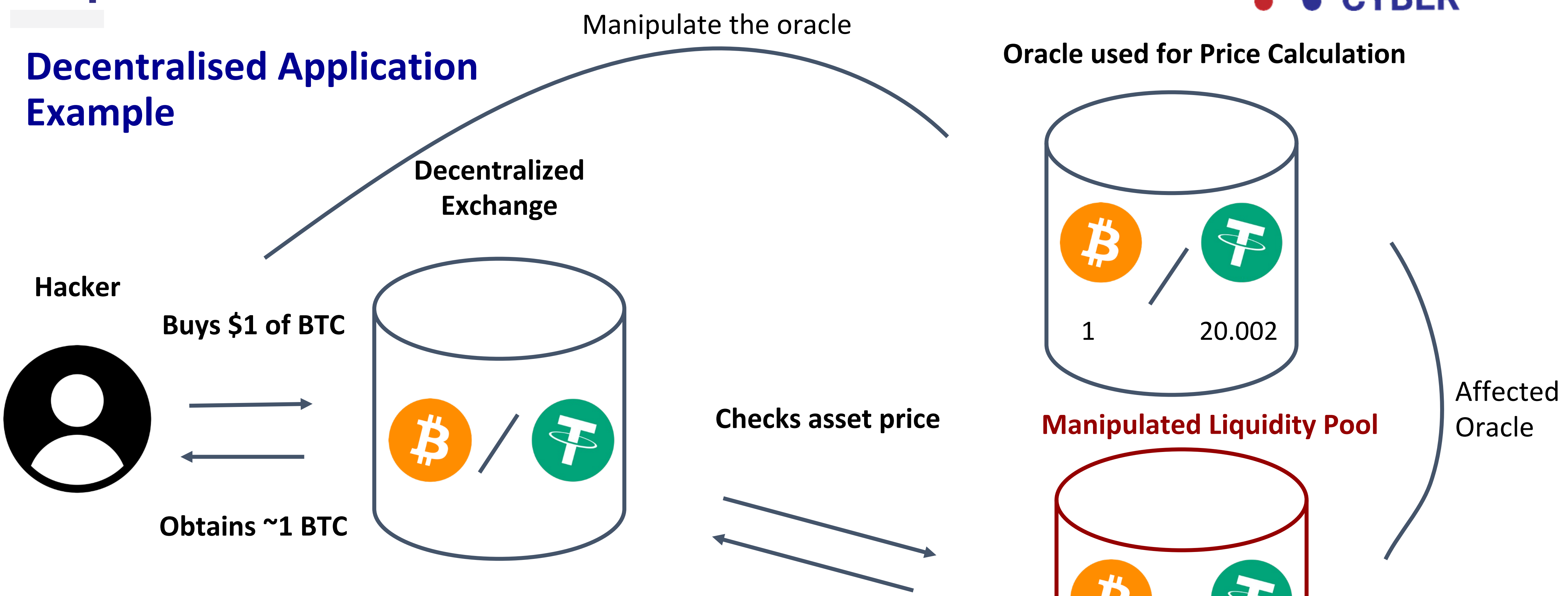
- Access restricted function (Elevation of privileges)
- Alter smart contract storage or behavior (Integrity)
- Financial loss

Mango Market Token Manipulation

PERFORMER	Avraham Eisenberg	**ANNÉE**	2021
VICTIM	Mango Markets	**PAYS**	NA
IMPACT	$117 Million lost.		
DESCRIPTION	Avraham Eisenberg manipulated the Mango Markets decentralized exchange by artificially inflating the price of its low-liquidity governance token, MNGO. He used a large initial deposit to buy and short MNGO simultaneously, causing the price to skyrocket. Eisenberg then borrowed against his inflated MNGO holdings, effectively draining the platform's assets. When the MNGO price inevitably collapsed, it was too late—Eisenberg had already extracted the majority of Mango Market’s valuable assets		

Exploits

Decentralised Application Example



Price of asset is calculated using the
Constant Function Market Maker K = X * Y

COMPONENTS ATTACKS

CONSENSUS LAYER (CONSENSUS PROTOCOLS)

VULNERABILITIES

- Design vulnerabilities
- Implementation vulnerabilities

IMPACTS

- DDOS (Availability)
- Groundless transactions (Integrity)
- Centralized Control transaction validation system (Availability)
- Double spending attack

HISTORICAL EVENTS

- Ethereum classic 51% attack

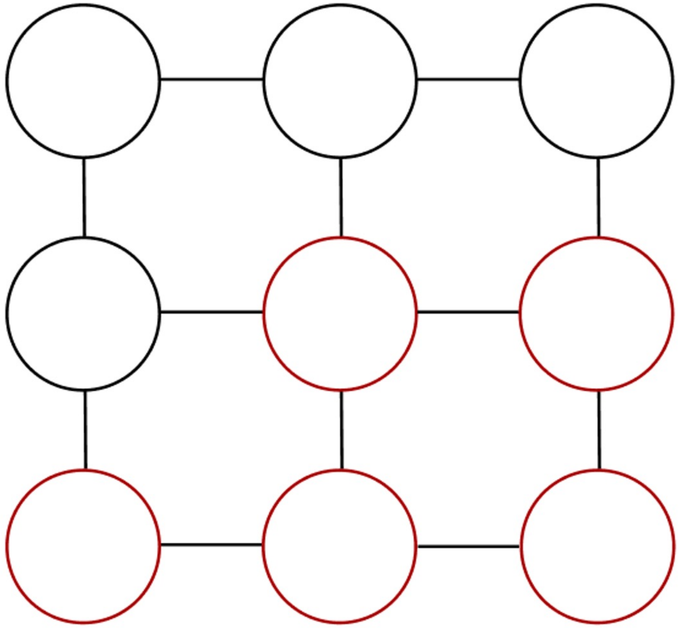
51% Attack on Bitcoin SV

PERFORMER	Unknown	**ANNÉE**	2021
VICTIM	Bitcoin SV	**PAYS**	N/A
IMPACT	Loss of miner and crypto value		
DESCRIPTION	The attack had a disruptive goal. Four attacks were perpetrated on July 2021 possibly due to two fundamental flaws on the network The first flaw is that Bitcoin SV is a Proof of Work based currency, meaning that fewer are on the network, weaker is the security which is usually the case for fork of a preexisting currency The second flaw is that the transaction fee is quite low, meaning that selling hash power to the network could not be profitable enough, leading to a loss of miner and by butterfly effect, a loss in the currency value. After this attack, roughly 14 blocks were reorganized, 570 000 transaction and 50% of the hash rate were lost, meaning than fewer people are mining on the network.		

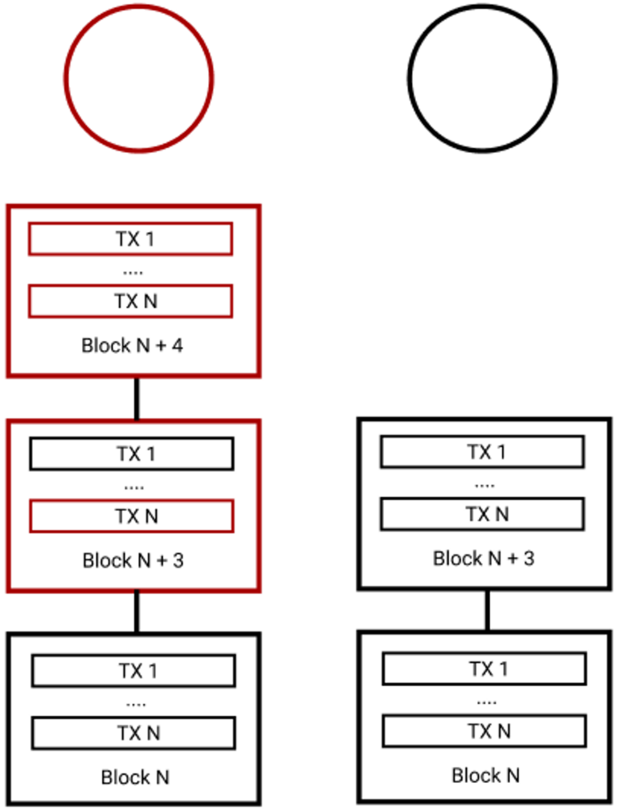
COMPONENTS ATTACKS

CONSENSUS LAYER EXAMPLE

51% Attack on Bitcoin SV



Malicious nodes with 55% of the validation power



Modified mined blocks and controlled new blocks

Smaller Chain

COMPONENTS ATTACKS

GOVERNANCE LAYER

VULNERABILITIES

- Design vulnerabilities related to on-chain type of governance
- Governance concentration between the hands of a
- small group of people

IMPACTS

- Service interruption
- Forks
- Theft of funds

HISTORICAL EVENTS

- Ethereum fork in 2016 and creation of Ethereum Classic
- BZX : Private key theft of administrators
- Beanstalk Farms : Flash loan to obtain majority of decision chair (draining all funds)

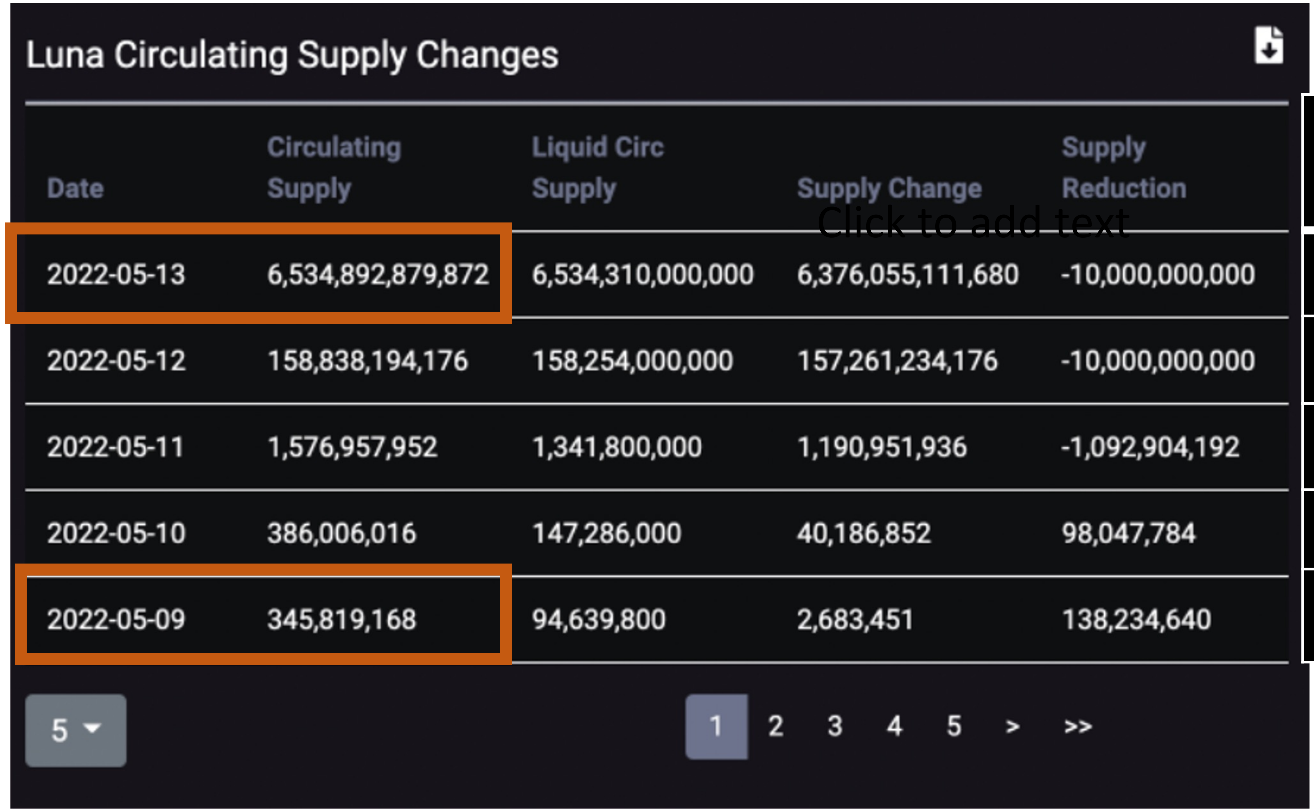
Terra on-chain vulnerabilities

PERFORMER	N/A	ANNÉE	2022
VICTIM	Terra	PAYS	South Korea
IMPACT	Service interruption		
DESCRIPTION	The TERRA blockchain has an on-chain Proof Of Stake type of governance. Its related token is the LUNA whose value dropped by 98% on the 9th of May 2022. The managers of the blockchain decided to temporarily stop the block production in order to avoid any rogue takeover of the blockchain. Indeed, Proof Of Stake type of governance means that decisions are likely to be taken by validators with delegation from the biggest token owners. As the LUNA price was very low, malicious actors had the opportunity to operate a massive purchase of a token, delegate their power of decision to a partner in crime and take control of the blockchain. The blockchain was eventually restarted after the new delegations functionality had been disabled.		

COMPONENTS ATTACKS

GOVERNANCE LAYER EXAMPLE

Terra on-chain vulnerabilities



Luna Circulating Supply Changes

Date	Circulating Supply	Liquid Circ Supply	Supply Change	Supply Reduction
2022-05-13	6,534,892,879,872	6,534,310,000,000	6,376,055,111,680	-10,000,000,000
2022-05-12	158,838,194,176	158,254,000,000	157,261,234,176	-10,000,000,000
2022-05-11	1,576,957,952	1,341,800,000	1,190,951,936	-1,092,904,192
2022-05-10	386,006,016	147,286,000	40,186,852	98,047,784
2022-05-09	345,819,168	94,639,800	2,683,451	138,234,640

Click to add text

Figure 1: Terra Analytics dashboard

Luna Price ($)
0.000167*
64*

Token Amount	Luna Price ($)
1	0.000167
345,819,168	57,760

* https://coinmarketcap.com/currencies/terra-luna/

COMPONENTS ATTACKS

NETWORK LAYER : NODES ON LAYERS 1

VULNERABILITIES

- Conception and implementation of blockchain clients software
- Misconfiguration and human flaws.

IMPACTS

- Potential for double spending attack.
- Leak of private keys (Confidentiality)

HISTORICAL EVENTS

- Eclipse attack
- Account Hijacking Attack

Exemple : DDOS on Solana Network

PERFORMER	Unknown	**ANNÉE**	2022

VICTIM	**Solana**	**PAYS**	NA
IMPACT	Solana 17 hours outage		

DESCRIPTION	● The DDoS attack on Solana took the network **down for hours** and ended only after the devs coordinated a **restart of the entire network.** ● Grape Protocol launched their IDO on Raydium, and **bots generated transactions that flooded the network**. ● At peak, there were **400,000 transactions per sec**, increasing the transaction pool size and making it harder for nodes to validate them. ● Eventually, **validators ran out of memory and crashed, going offline**.

COMPONENTS ATTACKS

NETWORK LAYER : NODES ON LAYERS 2

THREATS

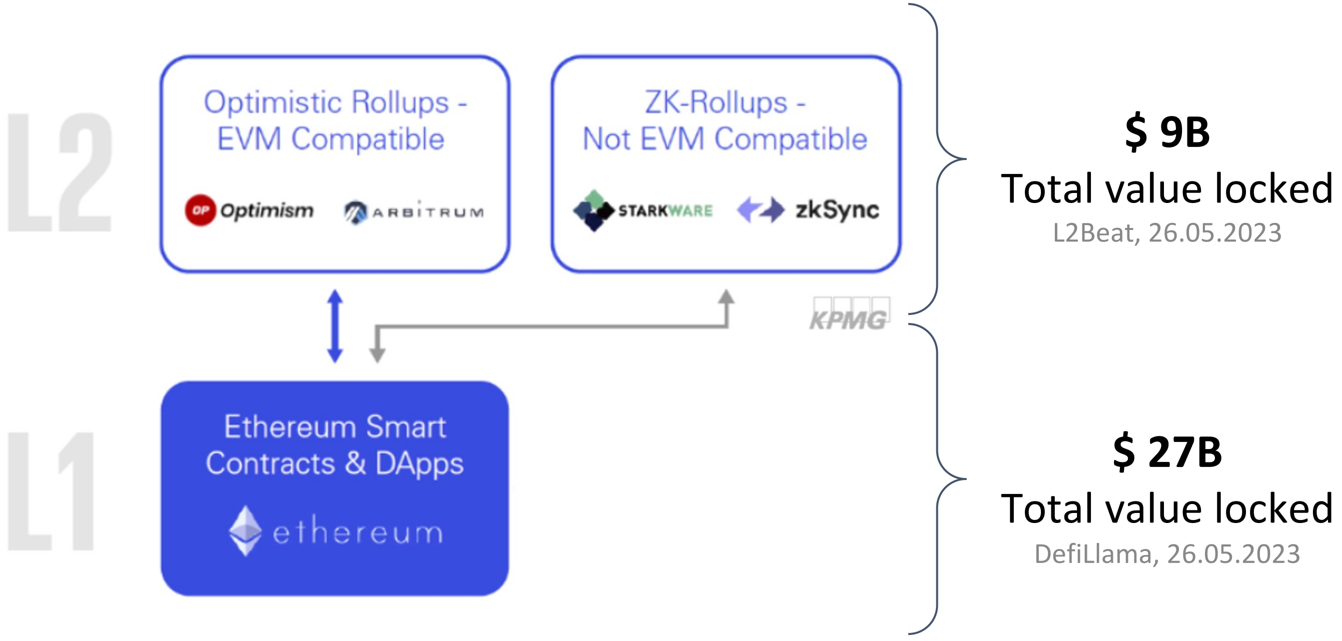
- Very new networks (2-year-old implementations)
- New machine instructions used on L2 software clients

IMPACTS

- Potential for double spending attack
- Decrease of scalability, Financial losses

DIFFICULTY

- Understand the cryptography behind zk-SNARKS/zk-STARKS proofs used on ZKR
- Understand the architecture and the information flow on OR



Ethereum Ecosystem

COMPONENTS ATTACKS

WALLET

VULNERABILITIES

- Flawed implementation of hierarchical deterministic wallets.
- Insecure storage or leaked seed phrases.
- Insecure storage or leaked private key.
- Insecure hardware wallet.
- Insecure custodian wallets.

IMPACTS

- Predictable wallet keys
- Funds and assets stolen

“Cold wallets”
i.e. hardware wallets

“Hot wallets”
i.e. online wallets

COMPONENTS ATTACKS

WALLET: Example of a COLD WALLET attack

PERFORMER	Kraken	**ANNÉE**	2019
VICTIM	**Trezor Hardware Wallet**	**PAYS**	
VULNERABILITY	**Inherent flaws within the microcontroller** used in the Trezor wallets		
DESCRIPTION	1. Removing the processor from the wallet and placing it in a socket **2. Dump of flash based on voltage glitching**, with two glitches. 3. Extracting the encrypted seed 4. Without countermeasures, the team can then **brute-force the 1-9 digit PIN** with a Python script 5. With the PIN, the team can access to the seed		

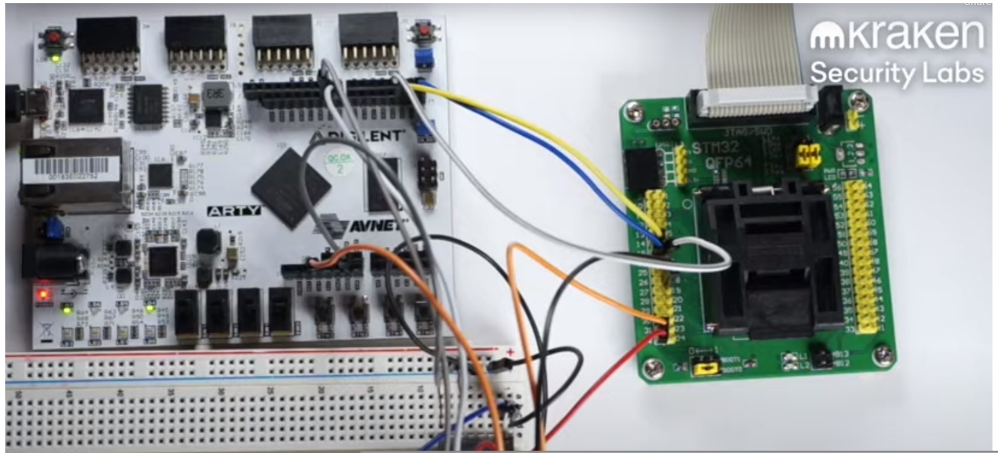


Fig 1 : Attack set

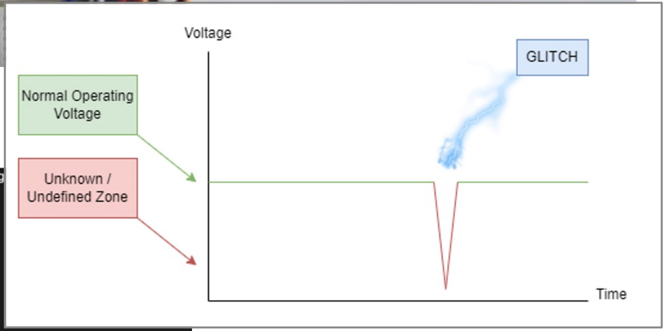
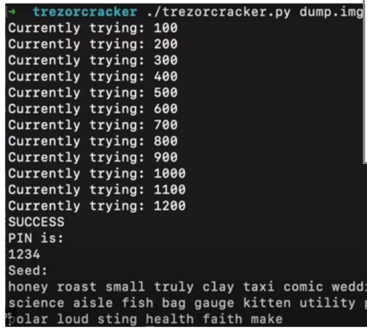


Fig 2 : Explanation of glitch attack



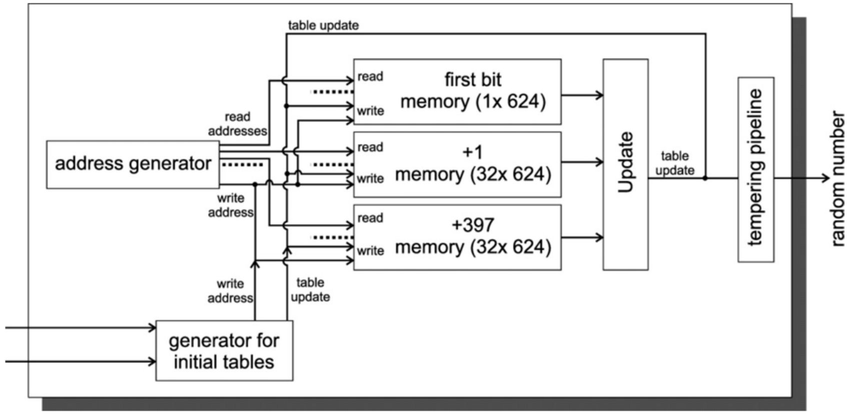
```
→  trezorcracker ./trezorcracker.py dump.img
Currently trying: 100
Currently trying: 200
Currently trying: 300
Currently trying: 400
Currently trying: 500
Currently trying: 600
Currently trying: 700
Currently trying: 800
Currently trying: 900
Currently trying: 1000
Currently trying: 1100
Currently trying: 1200
SUCCESS
PIN is:
1234
Seed:
honey roast small truly clay taxi comic wedding pumpkin
science aisle fish bag gauge kitten utility pact nose
polar loud sting health faith make
```

Fig 3 : Script to find the PIN & seed

COMPONENTS ATTACKS

WALLET: Example of a HOT WALLET attack

PERFORMER	Ledger Donjon	**ANNÉE**	2022
VICTIM	**Trust Wallet**	**PAYS**	France
VULNERABILITY	**Seed generation** of Trust Wallet was flawed, the **total entropy was only 32 bits**.		
DESCRIPTION	1. Flawed entropy generation: Trust Wallet's seed generation had low entropy. 2. Vulnerability discovery 3. Exploiting the vulnerability: Attacker **computes private keys from generated addresses**. 4. Gathering wallet addresses: Attacker **collects addresses created by Trust Wallet**. 5. Funds theft: Attacker could have drains wallets by **matching addresses and private keys**, but has reported the vulnerability. (around $ 30M at stake)		



Example of a Mersenne twister module (MT 19937)

Mersenne twisters, i.e. general-purpose pseudorandom number generator, were also used by Trust Wallet

Conclusions

The attacks which occurred these past ten years remind us that, despite its growth & popularity, the crypto-asset ecosystem and its security still **lack maturity**.

Therefore, Campus Cyber aims to actively participate in protecting this complex ecosystem.

Conclusion

Q&A

Thank you for your participation

See you in September

INSIDER.