Take The Money And Run

Decentralized Finance and the New Frontiers of Crime

Giovanni Vigna
UCSB
$whoami

• Computer Science Professor at UC Santa Barbara
• Co-founder CTO at Lastline, Inc. (acquired by VMware in 2020)
• Sr. Director of Threat Intelligence at VMware
• Founder of Shellphish
What Is DeFi?

“Decentralized finance offers financial instruments without relying on intermediaries such as brokerages, exchanges, or banks by using smart contracts on a blockchain”

- Wikipedia
Enthusiasts

- Provides unfettered access to financial instruments
- Takes out the middleman
- Takes away centralized control
- Uses code as the law
- It’s transparent
- It’s cheap(er)
Detractors

- It’s a scam that hurts people
- Transactions are irreversible
- Its value is not backed by a real economy
- It is not really decentralized
- It still has middlemen
- Most of its transactions are speculation and scams
- It’s bad for the environment
Letter in Support of Responsible Fintech Policy

“...we write to you urging you to take a critical, skeptical approach toward industry claims that crypto-assets (sometimes called cryptocurrencies, crypto tokens, or web3) are an innovative technology that is unreservedly good. We urge you to resist pressure from digital asset industry financiers, lobbyists, and boosters to create a regulatory safe haven for these risky, flawed, and unproven digital financial instruments and to instead take an approach that protects the public interest and ensures technology is deployed in genuine service to the needs of ordinary citizens”

https://concerned.tech/
A Wild Ride

LONDON, June 13 (Reuters) - The value of the cryptocurrency market on Monday fell below $1 trillion for the first time since January 2021, according to data site CoinMarketCap, reaching as low as $926 billion.

The global cryptocurrency market peaked at $2.9 trillion in November 2021, but it has faltered so far this year. It has lost $1 trillion in value in the last two months alone as investors ditched riskier assets in the face of high inflation and fears that interest rate raises by central banks will hamper growth.

Despite the market downturn, illicit transaction volume rose for the second consecutive year, hitting an all-time high of $20.6 billion. We have to stress that this is a lower bound estimate — our measure of illicit transaction volume is sure to grow over time as we identify new addresses associated with illicit activity, and we have to keep in mind that this figure doesn’t capture proceeds from non-crypto native crime (e.g. conventional drug trafficking involving cryptocurrency as a mode of payment).

For example, last year we published that we found $14 billion in illicit activity in 2021 — we’ve now raised that figure to $18 billion, mostly due to the discovery of new crypto scams.

It’s also worth keeping in mind that 43% of 2022’s illicit transaction volume came from activity associated with sanctioned entities, in a year when OFAC launched some of its most ambitious and difficult-to-enforce crypto sanctions yet. Crypto exchange Garantex, which accounted for the majority of sanctions-related transaction volume last year, is a great example. OFAC sanctioned Garantex in April 2022, but as a Russia-based business, the exchange has been able to continue operating with impunity. Transactions associated with Garantex or any other sanctioned crypto service represent, at the very least, substantial compliance risk for businesses that are subject to U.S. jurisdiction, including fines and potential criminal charges.

https://go.chainalysis.com/2023-crypto-crime-report.html
Ransomware

Conti was the biggest ransomware strain by revenue in 2021, extorting at least $180 million from victims. Believed to be based in Russia, Conti operates using the ransomware-as-a-service (RaaS) model, meaning Conti's operators allow affiliates to launch attacks using its ransomware program in exchange for a fee.

DarkSide is also notable, both for ranking second in 2021 in funds extorted from victims that we've been able to identify, and also for its role in the attack on oil pipeline Colonial Pipeline, one of the year's most notable ransomware attacks. The attack caused fuel shortages in some areas, which were exacerbated by subsequent panic buying as word of the attack's impact spread. The Colonial story serves as an important reminder of one reason ransomware attacks are so dangerous: They frequently target critical infrastructure we need to keep the country running — not just energy providers, but food providers, schools, hospitals and financial services companies as well.

However, the Colonial Pipeline attack also turned into a success story, as the U.S. Department of Justice was able to track and seize $2.3 million of the ransom that Colonial paid to DarkSide. We'll look more at how agents were able to do this later in the report.

<table>
<thead>
<tr>
<th>Top 10 ransomware strains by revenue</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conti</td>
<td>$200M</td>
</tr>
<tr>
<td>DarkSide</td>
<td>$150M</td>
</tr>
<tr>
<td>Phoenix Cryptolocker</td>
<td>$100M</td>
</tr>
<tr>
<td>REvil/Sodinokibi</td>
<td>$100M</td>
</tr>
<tr>
<td>LockBit</td>
<td>$100M</td>
</tr>
<tr>
<td>Hive</td>
<td>$100M</td>
</tr>
<tr>
<td>Ryuk</td>
<td>$100M</td>
</tr>
<tr>
<td>BlackMatter</td>
<td>$76M</td>
</tr>
<tr>
<td>Casa</td>
<td>$56M</td>
</tr>
<tr>
<td>Lightside</td>
<td>$43M</td>
</tr>
</tbody>
</table>

2021 ransomware activity summarized

Ransomware Revenue Down As More Victims Refuse to Pay

2022 was an impactful year in the fight against ransomware. Ransomware attackers extorted at least $456.8 million from victims in 2022, down from $765.6 million the year before.

As always, we have to caveat these findings by noting that the true totals are much higher, as there are cryptocurrency addresses controlled by ransomware attackers that have yet to be identified on the blockchain and incorporated into our data. When we published last year's version of this report, for example, we had only identified $602 million in ransomware payments in 2021. Still, the trend is clear: Ransomware payments are significantly down.

However, that doesn't mean attacks are down, or at least not as much as the drastic dropoff in payments would suggest. Instead, we believe that much of the decline is due to victim organizations increasingly refusing to pay ransomware attackers. We'll discuss this phenomenon more below, but first, let's look more at general ransomware trends in 2022.
Compare to the Good Ol’ Days…

- Zeus: 2007-2010
- “More than 100 people were arrested on charges of conspiracy to commit bank fraud and money laundering, over 90 in the US, and the others in the UK and Ukraine. Members of the ring had stolen $70 million.”

We Need to Talk About the Blockchain.
Blockchains, Blocks, and Transactions

• Append-only distributed security ledgers
• Consensus protocol allows for agreement about the contents of the blocks
• Most of the times, the contents of the block are a list of transactions

https://en.wikipedia.org/wiki/Blockchain
L1 Blockchains (and their coins)

- Bitcoin and Ethereum account for the vast majority of the market cap
- Ethereum
  - Supports smart contracts
  - In September 2022, moved from Proof-of-Work to Proof-of-Stake

<table>
<thead>
<tr>
<th>Layer-1 coins</th>
<th>Price</th>
<th>Market cap</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 Bitcoin</td>
<td>$28,200.64</td>
<td>$541.96 billion</td>
</tr>
<tr>
<td>#2 Ethereum</td>
<td>$1,801.56</td>
<td>$219.81 billion</td>
</tr>
<tr>
<td>#3 BNB</td>
<td>$314.35</td>
<td>$44.93 billion</td>
</tr>
<tr>
<td>#4 XRP</td>
<td>$0.5281</td>
<td>$26.55 billion</td>
</tr>
<tr>
<td>#5 Cardano</td>
<td>$0.3826</td>
<td>$13.40 billion</td>
</tr>
<tr>
<td>#6 Dogecoin</td>
<td>$0.08013</td>
<td>$10.96 billion</td>
</tr>
<tr>
<td>#7 OKB</td>
<td>$41.37</td>
<td>$9.99 billion</td>
</tr>
<tr>
<td>#8 Polkadot</td>
<td>$6.326</td>
<td>$7.67 billion</td>
</tr>
<tr>
<td>#9 Solana</td>
<td>$20.63</td>
<td>$7.49 billion</td>
</tr>
<tr>
<td>#10 Litecoin</td>
<td>$92.95</td>
<td>$6.59 billion</td>
</tr>
</tbody>
</table>

https://coinranking.com/coins/layer-1
Smart Contracts

• Programs running on top of Ethereum blockchain
• Execute as bytecode on top of Ethereum Virtual Machine (EVM)
• Typically developed in higher-level languages such as Solidity
• Power DeFi applications, tokens, games, collectibles, …
Ethereum Transactions

• Transfer Ether from address A to address B
• Deploy a smart contract on the block chain
• Invoke a function in a deployed smart contract

• Transactions are submitted to a public mempool
• There are ways to bypass the mempool by using Flashbots
Block Producers and MEV

• Block Producers: Miners (PoW) and Validators (PoS)
• “Maximal Extractable Value (MEV) refers to the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, and changing the order of transactions in a block.” (https://ethereum.org/en/developers/docs/mev/)
• Bots and producers compete to determine the selection and ordering of transaction in a block
• Typical example: Arbitrage (more on that later)
Tokens

- Token contracts are used to track ownership of assets
- ERC-20 standardizes the interface for fungible token contracts
- ERC-721 standardizes the interface for non-fungible token contracts

https://etherscan.io/tokens
Centralized Exchanges

• Ramp-in
  • Transfer money from a bank account into Ether

• Ramp-out
  • Transfer Ether into actual money in a bank account

https://coinmarketcap.com/rankings/exchanges/
Where’s the Money?
Make the Money

• Lending (Flash loans!)
  • AAVE, Compound

• Derivatives
  • dYdX

• Yield Farms
  • Curve

• Decentralize Exchanges
  • UniSwap, SushiSwap
Automated Market Makers (AMMs)

- Based on liquidity pools
  - They do not maintain an order book
- Exchange price is automatically determined
  - For example, the product of the two assets constant
- Created from smart contract factory
Arbitrage

- Opportunity caused by the same asset having different prices on different exchanges
- Multiple exchanges in a single transaction
- Analysis performed off-line
- Execution by relayer smart contract
How Much Arbitrage?

- We analyzed 28 months of data (~1 billion transactions)
- Identified 4,070,938 arbitrage transactions
  - 90+% only 2-3 exchanges involved
  - 90+% pivoted on Wrapped ETH
  - Uniswap v2 and v3 and SushiSwap are the most involved AMMs
- $321 millions in profit
  - Top bot 1: $37M
  - Top bot 2: $31M
  - Top bot 3: $26M

A Large Scale Study of the Ethereum Arbitrage Ecosystem

Robert McLaughlin, Christopher Kruegel, Giovanni Vigna
University of California, Santa Barbara
{robert349, chris, vigna}@cs.ucsb.edu

USENIX Security 2023
Transaction Order Matters

- Bots monitor the mempool
- Identify transactions that might create an arbitrage opportunity
- Attempt to put an arbitrage transaction right after trade (back-running)
- Might use Flashbots to avoid a bidding war
Transaction Order Matters

• Sandwich attacks
  • Identify a target transaction that might change the valuation of an asset
  • Attempt to put a transaction before and one afterwards to take advantage of the change

• Front-running attacks
  • Identify a profit-making transaction
  • Attempt to put a similar transaction (with a different beneficiary) before the target transaction
Take the Money

• Stolen funds
  • Hacks
  • Wallet compromise

• Scams
  • Ponzi schemes
  • Pig butchering/romance scams
  • Investment scams

• Ransomware

• Rag pulls
Hacks! Hacks!

- Traditional hacks
  - Compromised credentials
  - Unauthorized access

- Bridge hacks
  - Custodian attacks
  - Debt issuer attacks
  - Communicator attacks

- Protocol hacks
  - Oracle manipulation
  - ...

https://rekt.news/
2022 was the biggest year ever for crypto hacking, with $3.8 billion stolen from cryptocurrency businesses. Hacking activity ebbed and flowed throughout the year, with huge spikes in March and October, the latter of which became the biggest single month ever for cryptocurrency hacking, as $775.7 million was stolen in 32 separate attacks.

North Korea-linked hackers break theft records yet again: $1.7 billion stolen
North Korea-linked hackers such as those in cybercriminal syndicate Lazarus Group have been by far the most prolific cryptocurrency hackers over the last few years. In 2022, they shattered their own records for theft, stealing an estimated $1.7 billion worth of cryptocurrency across several hacks we've attributed to them. For context, North Korea's total exports in 2020 totalled $142 million worth of goods, so it isn't a stretch to say that cryptocurrency hacking is a sizable chunk of the nation's economy. Most experts agree the North Korean government is using these stolen to fund its nuclear weapons programs.

$1.1 billion of that total was stolen in hacks of DeFi protocols, making North Korea one of the driving forces behind the DeFi hacking trend that intensified in 2022. North Korea-linked hackers tend to send much of what they steal to other DeFi protocols, not because these protocols are effective for money laundering — they're actually quite bad for money laundering given their increased transparency compared to centralized services — but rather because DeFi hacks often result in cyber criminals acquiring large quantities of illiquid tokens that aren't listed at centralized exchanges. The hackers therefore must turn to other DeFi protocols, usually DEXes, to swap for more liquid assets.

https://go.chainalysis.com/2023-crypto-crime-report.html
Ronin Network Hack

- Side chain
- Required consensus of 5 out of 9 servers for transfer
- 4 servers were managed by the same entity
- A fifth entity had temporary delegated the right to sign
- The hacker stole $624M
- The team didn’t notice until a week later…
Nomad Bridge Hack

- Faulty update allows for address 0x0 to be authorized as root
- First attempt to compromise failed (and cost $350K in gas!)
- Second attempt succeeded and was followed by everyone else
- $190M stolen in 2.5 hours as a result

https://defillama.com/protocol/nomad
Wormhole Hack

• Wormhole is a token bridge between Ethereum and Solana
• A bug allowed an attacker to provide both a signature and the contract needed to verify the signature
• This allowed for the minting of wrapped Ethereum on Solana, which was then transferred back to Ethereum
• $326M were lost
Take the Money and Launder It

• Once the money is stolen, it can be tracked, requiring laundering
• Money can be laundered by mixers, exchanges, DeFi applications, games, etc.
• DeFi application have seen a substantial increase as a means to launder cash
• Tornado Cash is a mixer that uses Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) to allow a user to deposit an Ether amount and then extract it without the possibility to link the two operations
Overall, illicit addresses sent nearly $23.8 billion worth of cryptocurrency in 2022, a 68.0% increase over 2021. As is usually the case, mainstream centralized exchanges were the biggest recipient of illicit cryptocurrency, taking in just under half of all funds sent from illicit addresses. That’s notable not just because those exchanges generally have compliance measures in place to report this activity and take action against the users in question, but also because those exchanges are fiat off-ramps, where the illicit cryptocurrency can be converted into cash.
US Fights Back

• The US Office of Foreign Assets Control (OFAC) has put exchanges (e.g., Russia-based Suex and Chatex, in September 2021) on the Specially Designated Nationals and Blocked Persons (SDN) list

• In May 2022, OFAC put Blender.io on the SDN list

• In August 2022, OFAC put Tornado Cash on the SDN list
  • Used to launder Lazarus group’s $455M heist
Securing Smart Contracts

• “The code is the law”
• What if the code is broken?
• What if the source code is not even public?
• Problems
  • Function visibility
  • Reentrancy and order of transactions
  • Timing
  • Randomness
Audits and Bug Bounties

• Ecosystem of companies that perform audits
  • Trail of Bits, ConsenSys Diligence, Certik, Hacken, OpenZeppelin, …

• Provide no guarantees

• Bug bounties are a way to incentivize responsible disclosure
  • Immunefi, HackenProof
Automated Vulnerability Analysis

• Combination of static and dynamic analysis
• Small code sizes make it possible to adopt resource-heavy approaches
• Execution is limited by gas price
• Memory models are simpler
• All the code is available
Reentrancy

- Bank contract allows withdrawal of Ethers by users
- The `withdraw()` function transfers the amount through an external call
- After the call returns, user’s balance is updated.
- A user implements `getEthers()` to withdraw 100 Ethers from the Bank
- She also invokes `bank.withdraw(100)` within her `fallback()` function as well
Reentrancy

Attacker

```javascript
getEthers() {
    bank.withdraw(100)
}

payable() {
    bank.withdraw(100)
}
```

Bank

```javascript
withdraw() {
    if (accounts[msg.sender] >= amount)
        msg.sender.call.value(amount)
    accounts[msg.sender] -= amount
}
```
Reentrancy

```
getEthers() {
    bank.withdraw(100)
}

payable() {
    bank.withdraw(100)
}
```

```
Bank
withdraw() {
    if (accounts[msg.sender] >= amount)
        msg.sender.call.value(amount)
    accounts[msg.sender] -= amount
}
```
Reentrancy

**Attacker**

```javascript
getEthers() {
    bank.withdraw(100)
}

payable() {
    bank.withdraw(100)
}
```

**Bank**

```javascript
withdraw() {
    if (accounts[msg.sender] >= amount)
        msg.sender.call.value(amount)
        accounts[msg.sender] -= amount
}
```

- **Call Reentrancy**
  - [1] `getEthers()` calls `withdraw()`
  - [2] `withdraw()` calls `msg.sender.call.value(amount)`
  - [3] `msg.sender.call.value(amount)` calls `withdraw()` again

- **Reentrant Call**
  - Step 4: `withdraw()` calls itself multiple times through the stack, potentially leading to a reentrant error.
Reentrancy

```javascript
getEthers() {
    bank.withdraw(100)
}

payable() {
    bank.withdraw(100)
}
```

### Diagram

**Attacker**
- getEthers() { bank.withdraw(100) }
- payable() { bank.withdraw(100) }

**Bank**
- withdraw() {
  - if (accounts[msg.sender] >= amount)
    - msg.sender.call.value(amount)
    - accounts[msg.sender] -= amount
```
**SAILFISH: Vetting Smart Contract State-Inconsistency Bugs in Seconds**

Priyanka Bose, Dipanjan Das, Yanju Chen, Yu Feng, Christopher Kruegel, and Giovanni Vigna

University of California, Santa Barbara

{priyanka, dipanjan, yanju, yufeng, chris, vigna}@cs.ucsb.edu

*IEEE Symposium on Security and Privacy, May 2022*
Confused Deputy

A

B
Confused Deputy

A: Can I have the key?

B: NOPE
Confused Deputy
Confused Deputy

A

Ask for the key and give it to me!

C

B
Confused Deputy

A

C

I need the key!

B
Confused Deputy

A

C

Oh, sure!

B
Confused Deputy

A

C

Thanks!

B
Confused Deputy

A

Here the key, have a nice day!

C

B
Confused Deputy

A

C
Confused Deputy

B
Target

But... I trusted you...
Confused Contract
Confused Contract

msg.sender = A
tx.origin = A

CALL

iTX
Confused Contract

msg.sender = A
tx.origin = A

Data provided must be coming from A!
Confused Contract

Alice

MyBot

MyBank

MyBot:

Bob:

MyBot: 

Bob: 

MyBot: 

Bob: 

MyBot: 

Bob: 

MyBot: 

Bob: 

MyBot: 

Bob:
Confused Contract

msg.sender = A
tx.origin = A
func: transfer
to : Bob
val: 2

Transfer of funds (benign)
Confused Contract

msg.sender = A
tx.origin = A
func: transfer
to : Bob
val: 2

Transfer of funds
(benign)
Confused Contract

Confused contracts are a type of smart contract that can lead to unexpected behavior due to their self-referential nature. In the case of MyBot and MyBank, Alice sends a transaction (TX) to MyBot, and MyBot, thinking it is being sent to Alice, transfers the funds back to Alice.

Transfer of funds (benign)
Confused Contract

Transfer of funds (benign)

msg.sender = A
tx.origin = A
func: transfer to : Bob
val: 2

msg.sender = myBot
tx.origin = A
func: transfer to : Bob
val: 2
Confused Contract

Transfer of funds (malicious)
Confused Contract

msg.sender = M
tx.origin = M
func: transfer
to: Mallory
val: 3

Transfer of funds (malicious)
Confused Contract

Transfer of funds (malicious)
Confused Contract

msg.sender = M
tx.origin = M
func: transfer
to: Mallory
val: 3

msg.sender = myBot
tx.origin = M
func: transfer
to: Mallory
val: 3

Mallory:

MyBot:

MyBank:

Transfer of funds (malicious)
Confused Contract

MyBot:
msg.sender = M
tx.origin = M
func: transfer
to: Mallory
val: 3

Mallory:
iTX
msg.sender = myBot
tx.origin = M
func: transfer
to: Mallory
val: 3

Transfer of funds (malicious)
KAI

- 2,000,000+ smart contracts
  - Deployed between December 2020 → D€
- 529 potential Confused Contracts
  - 84 warnings Confused Contract + Contract Target_
- 13 working exploits for a total value of more than $1,000,000
Call To Action

• We need better tools to analyze smart contracts
  • Dynamic symbolic execution
  • Static analysis
  • Model checking
  • Fuzzing
  • Decompilers

• We need more people looking at smart contracts
  • Start breaking stuff (responsibly) and collect amazing bug bounties!

• We need ways to recover stolen funds
  • Prevent money laundering
  • Reversible tokens (ERC-20R and ERC-721R proposal by Stanford researchers)
Conclusions

• The DeFi ecosystem is a fascinating new target for security research
  • For both enthusiasts and detractors!
• Tools are primitive, human expertise is lacking
• If DeFi truly becomes the future of finance, we need to do something, or we are doomed… … and maybe it’s a good thing!
NFTs

• Of course, we didn’t have the time to talk about NFTs…
Thanks!

Questions to vigna@ucsb.edu