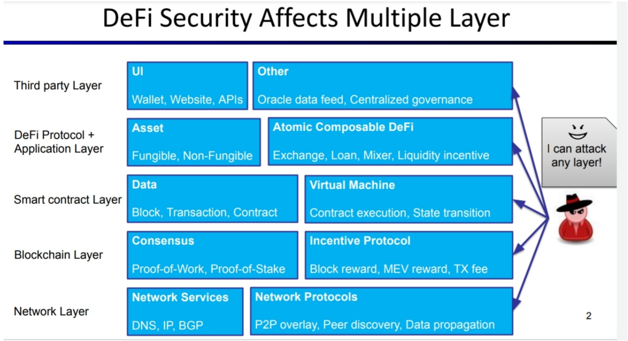
DeFi Attacks - part 1

Shymaa M. Arafat
shymaa.arafat@gmail.com, shar.academic@gmail.com

Crypto-currencies based on permissionless blockchains such as Bitcoin & Ethereum have gained more attention in the last few years since they increase financial inclusion and ease anonymity for those who needs it. Ethereum as a poineer of the EVM design and the ability to use smart contracts, followed by all EVM like cryptocurrencies, have excelled at financial services, that the word DeFi became widely used exceeding the traditional finance scope to a variety of applications including almost every aspect of life. However DeFi is not risk free, and naturally will be susceptible to the attacks of all involved areas and what evolves from their join,Fig.1; you may also have a look at this running record of all reported complaints of stolen money [1].



DeFi Security Affects Multiple Layer

Third party Layer
UI
Wallet, Website, APIs
Other
Oracle data feed, Centralized governance

DeFi Protocol + Application Layer
Asset
Fungible, Non-Fungible
Atomic Composable DeFi
Exchange, Loan, Mixer, Liquidity incentive

Smart contract Layer
Data
Block, Transaction, Contract
Virtual Machine
Contract execution, State transition

Blockchain Layer
Consensus
Proof-of-Work, Proof-of-Stake
Incentive Protocol
Block reward, MEV reward, TX fee

Network Layer
Network Services
DNS, IP, BGP
Network Protocols
P2P overlay, Peer discovery, Data propagation

I can attack any layer!

Fig.1: from [17] interacting with DeFi goes through all these layers, and thus users are succeptible to the vulnerabilities in each layer

Your interface device

When entering a permissionless network environment, especially holding money, you have to be your own guard and be aware of common network security attacks towards your device interface like SIM-Swap[2,3,4], address spoofing [5], DoS,….etc.

Application & Protocol Exploit

Applications and protocols that you invest your money through are smart contracts; i.e., written programs that an adversary can find inside it a semantic vulnerability to attack [6]. Examples include a missed check that the attacker can use to enter wrong value and drain locked money, put the protocol in an infinite loop,..etc.

-The AMA between Arthur Gervais & Vivik Nair in [7] discussed how the considerably long 10min duration between price oracles in ***iron coin*** and missing a boundary check for the maximum allowed value in ***Terra*** were protocol exploits that led to the spiral effect; I had a straight forward thought at the time, why not iron protocol prevents more than one exchange for the same key (or certain money threshold) within one oracle interval, of course it won't prevent the same attackers from generating multiple key pairs, but at least it will consume more time and putting a threshold on value exchanged no matter what key will solve it.

-Another interesting protocol attack was mentioned during the chat with Curve founder [8], a somewhat snippy attack on ***Uniswap v3***; if a Bot censored a large exchange is about to happen, it could narrowly deposit its liquidity in the interval where the trade is going to happen, then it can guarantee taking all the fees for having the deepest density in this region (while providing much less liquidity than he would need in v2); finally if the attacker traded his profits in another DEX, it would be like he took away Uniswap 0.3% fee from the censored trade[1] instead of paying it. Arthur Gervais colleagues at the Imperial collage formalized a definition for the attack as ***JIT Just in Time liquidity*** attack in a recent paper[9]; however they don't find it as profitable as Michael Egorov expected (0.007% instead of 0.3%), I think maybe Uniswap v3 modified the protocol in the time between to make it less profitable probably by imposing more constrains on the amount of liquidity added.

Smart Contract Vulnerabilities

Smart contracts as programs written to be executable on EVM model (and compatible s), were found to have some known coding vulnerabilities that developers have to avoid; material for such attacks are found under the title "*Practical Smart Contract Security*", from which I refer the reader to [10,11]. Also a glossary is available at [12], ***Smart Contract Weakness Classification Registry (SWCR).***

Exit-spam & Rug-Pull

Since there's money involved, users should also be aware of exit-spam & Rug-Pull attacks where fake or fraud applications simply runaway with your money[13]. I think most existing DeFi lawsuits are actually about the fine grain between messing an exploit as a developer, or a financial expert, or deliberately running an API or DAO to drain people money. A common practice to protect yourself is to investigate the reputation of a DAO or API before you invest your money in, especially there are available audit records[14]. [15,16] include some applications tryto protect from Rug-Pull attack, while [17] provides indepth analysis.

Blockchain layer attacks, like vulnerabilities in consensus protocols or rewarding mechanisms, is beyond the scope of this article; I encourage the interested reader to search for some POS attacks, like ***nothing at stake*** and ***long range*** attack.

Network Layer Attacks & Propagation Time

There are also some attacks that exploit the difference in time TXs take (coming from different

[1] Although this attack depends on censoring TXs, and thus could be classified as front-running that we will discuss later, I preferred to put it here since it's caused mainly by Uniswap v3 AMM formulas; ie., a protocol exploit.

locations around the globe) to propagate through the network layer before reaching any destination pool, Fig 2.

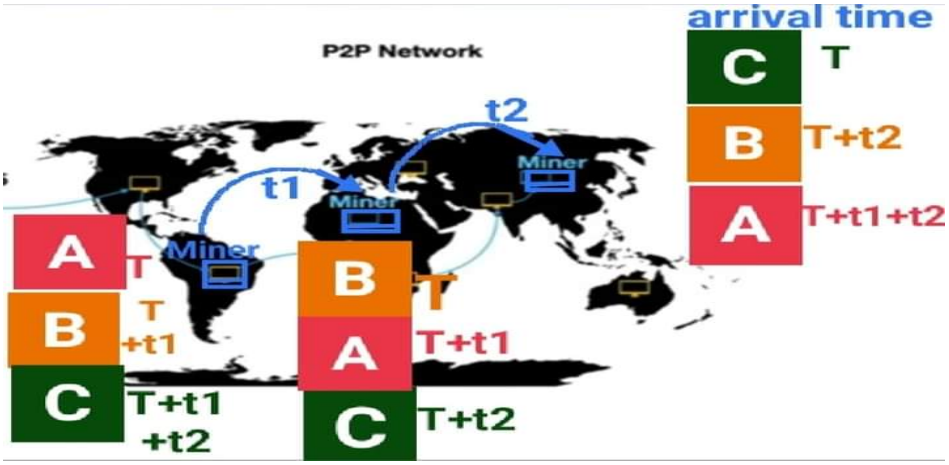


Fig.2: a diagram showing how would 3 TXs hypothetically assembled at the same time in different locations could get ordered differently according to the pool location

The lecture [18] is a clear & reliable source to understand such attacks and how to avoid them. To summarize, the main vulnerability comes from the fact that quite distant users (probably in countries with less crypto usage ratios, and thus less full nodes) usually have to choose between fewer number of service providers; a malicious service providers or a malicious hacker monitoring the one or two service providers can act as a ***spy node*** and have almost the same miner powers that I will describe in the following section.

Similarly such adversary can easier isolate a faraway victim in a DoS attack or deceive him into a double spending, what is called ***eclipse attacks***; when this attack was first discovered on Bitcoin 2015, it required the attacker to possess a lot of Bots, the reverse of the Uniswap v3 case here technology advancement made the attack possible with 1 connection only.

In Dec 2022 Crypto Economic workshops, *Flashbots* announced their new protocol, ***SUAVE***, [19], they stated that one of its goals is to achieve geographic diversity (which means equal chances for TXs suffering longer propagation delay); as the mitigations described in [18] they also said maybe we need to accept 15 secs between blocks to leave about 7 secs for arrival as in internet partial synchronization[2] assumption.

Economic Attacks

[2] 7 here is the alpha in “assume synchronous within alpha" model, if you follow Tim Roughgarden Foundation of Blockchains lectures

Another kind of attacks that I prefer to call Economic Attacks or Market manipulation attacks since most of them mirror a corresponding scenario that could happen, even if little differently in regular stock markets or fiat currency exchange s if someone gained access to secret informations to act before everyone else or by the brokers themselves).

In traditional finance if a large amount of asset X is to be sold to get asset Y, anyone who had access to the information (from the seller opponents to the brokers themselves) could use the info to gain some profit possibly affecting the profit of the original operation. The situation gets worse in the DeFi automated environment where TXs happen in a fraction of second, and there are programmable bots that search for such opportunities, hence came the term Ethereum as "***a dark forest***", [20]; infact the following attacks applies to almost any blockchain and sometimes could even happen across chains.

When transactions wait in a Mempool to get selected by miners according to their fees, it is possible for an adversary to use the publicly available information of the transaction contents to catch the profitable opportunity. With a higher transaction fee the adversary can get his TX to be minted first! what we call ***front-runnig***. Then for our (X,Y) exchange example, if the victim TX ran afterwards, it will be executed on the new AMM prices with Y becoming more expensive; according to [21], 20% of Uniswap v3 TXs would have been more profitable if placed earlier in the block. Another side effect is raising the average rate of transaction fees for ordinary users that have nothing to do with the going competition; what is sometimes called ***gas wars***.

Examples[3] extend currency exchange to include cases like Alice trying to register a domain name and Mallory registering it first; Alice trying to submit a bug to receive a bounty and Mallory stealing it and submitting it first; Alice trying to submit a bid in an auction and Mallory copying it; Alice and Mallory are competing to liquidate a loan; or even Alice and Mallory are competing on a free airdrop NFT[4], or to be the first winner of a game (happened in the Fomo3d game[5] 2018).

Now, above all “Mallory alike" adversaries comes ***miners***; they have the highest privilege to impose any displacement, insertion, or suppression they like on the order of TXs inside their blocks. Miners can copy-paste any profitable TX and put theirs first, sandwich the victim TX inside 2 TXs of their own,.., and even more. Such attacks fall under the global title ***BEV*** (***Block Extracted Value***) and the more widely used name ***MEV*** (***Miner Extracted Value***), which is now recently preferred to stand for ***Maximal Extracted Value*** to include POS blockchains cases when there are no miners (there are proposers & builders); Fig.3 from [22]. An on the fly protection, that I will defer its analysis to part-2, is to put the TXs encrypted in the Mempool then reveal them only after the miner is committed to include them in a certain order in the block,

[3] On a case by case basis in those example, Alice TX could become less profitable, or completely useless or invalid due to the attack.

[4] Fair distribution of NFT free airdrops is a standalone subject of many studies; ie, beyond the scope of this article, the point is if the selection criteria applies to Alice (the one who sends first, the one who sends more,... etc) and Mallory tried to steal the chance.

[5] The Fomo3d game attack happened in 2018, https://www.apriorit.com/dev-blog/556-fomo3d-vulnerability

what is called ***commit-then-reveal***; for POS there is ***Proposer Builder Separation*** through Relays (presentation A in [19]), ***PBS***.

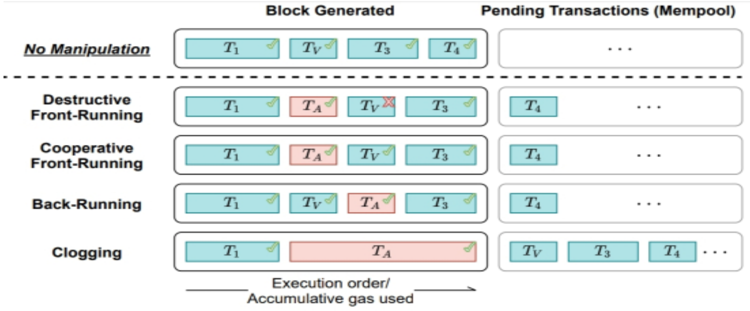

Block Generated
Pending Transactions (Mempool)
No Manipulation
Destructive Front-Running
Cooperative Front-Running
Back-Running
Clogging
T_1
T_V
T_3
T_4
T_A
. . .
Execution order/ Accumulative gas used

Figure 1: Visualization of the four types of adversarial transaction ordering strategies. T_V is the victim and T_A the adversarial transaction. We assume that T_1 to T_4, are included in the next block in their sequence.

Fig.3: a figure summarizing MEV/BEV attacks from [19]

I think this enough for part-1, I will leave your thoughts open about MEV (till part-2) and point you out to their 2022 numbers in one DEX only, Uniswap, [23,24].

I also remind you that this is still not everything you need to know; there are more attacks of economic nature, there are more attacks that I will try to cover in following parts like ***pump-and-dump*** attacks, attacks involving ***flashloans***, and ***oracle manipulation*** attacks. There are also ***cross-chain*** variations that happen across different blockchains (think of front running on a different Blockchain, or think of attacks on bridges,..).

References

[1]https://www.chainabuse.com/reports, last accessed 21/6/2023

[2]https://www.coindesk.com/business/2020/12/23/from-sim-swaps-to-home-invasion-threats-ledger-leak-has-cascading-consequences/

[3]https://en.m.wikipedia.org/wiki/SIM_swap_scam

[4]https://www.wired.com/story/sim-swap-attack-defend-phone/

[5] https://youtu.be/__8sGeBVYrM

[6]https://www.coindesk.com/markets/2020/12/28/who-insures-the-insurer-cover-protocol-attack-exposes-defis-promise-and-peril/

[7] Arthur Gervais & Vivik Nair, Berkeley DeFi MOOC 2022, AMA; https://youtu.be/-tNSqrmMSNg, last accessed 21/6/2023

[8] Arthur Gervais & Michael Egorov founder of Curve Finance, DeFi MOOC 2021 Fireside chat, mins 1:35-1:39; https://youtu.be/bNn0kCU7mrY

[9] Xihan Xiong, Zhipeng Wang, Michael Huth, "*Demystifying Just-in-Time (JIT) Liquidity Attacks on Uniswap V3*"; https://eprint.iacr.org/2023/973

[10] Samczsun, “*Practical Smart Contract Security*", Berkeley DeFi MOOC 2021, lec 12; https://youtu.be/pJKy5HWuFK8

[11]https://consensys.github.io/smart-contract-best-practices/attacks/

[12] *Smart Contract Weakness Classification Registry*, https://swcregistry.io/, last accessed 20/6/2023

[13] “*DeFi Scam Types*", University of Nicosia DeFi MOOC, BLOC529–03-s23,session 11; https://youtu.be/eLRJOhAyPpk

[14]https://www.binance.com/en/feed/post/152495, last accessed 21/6/2023

[15]https://www.bsc.news/post/rug-pull-defense-101-essential-tools-to-keep-your-web3-investments-secure, last accessed 21/6/2023

[16]https://medium.com/coinmonks/rug-pull-cons-hurt-nft-credibility-63df82fd75e4, last accessed 15/6/2023

[17] "*Understanding RUG PULLS: an in-Depth Behavioral Analysis of Fraudulent NFT Creators*", arXiv:2304.07598v1 [cs.CR] 15 Apr 2023

[18]Arthur Gervais, “*Network Layer Security* ", Berkeley DeFi MOOC 2021, lec:13.1–13.3; https://youtu.be/GIHa2GQJY1k, last accessed 21/6/2023

[19] Phillip Daian, Flashbots, “*MEV Desiderata: Selected Trillion Dollar Questions?*”, Columbia Crypto-Economics Workshop 12/2022, session 1, presentation 1B; https://youtu.be/175fuv2RJUo

[20] Dan Robinson and Georgios Konstantopoulos, "*Ethereum is a Dark Forest*",https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest, last accessed 21/6/2021

[21] Dan Robinson, Berkeley Web3 MOOC 2022, https://rdi.berkeley.edu/course/entrepreneurship-in-web3, lec2, min 1:11; https://www.youtube.com/live/YWo2zM-0SDI

[22] Arthur Gervais,Liyi Zhou, et al, “*Quantifying Blockchain Extractable Value: How dark is the forest?*”, Jan2021; https://arxiv.org/abs/2101.05511

[23]https://medium.com/@eigenphi/mevs-impact-on-uniswap-c36c7dfbd3d4, last accessed 20/6/2023

[24]https://dune.com/alexth/uniswap-v3-mev-activity