Design Secure DeFi Systems to Enable Financial Inclusion

Ken Huang, Chair, Blockchain Security Working Group, Cloud Security Alliance, GCR
William Zhang, Security Architecture Lead, The World Bank Group

Abstract

Decentralized Finance (DeFi), powered by blockchains and on-chain smart contracts, has grown into a significant economy that includes exchanges, borrowing/lending, yield farming, liquidity mining, margin trading, derivatives, and more. DeFi has provided some level of inclusiveness due to the public and permissionless nature of blockchain.

However, the majority of DeFi projects are built without strong cyber security processes and procedures that you would expect from enterprise application development such as the DevSecOps process. As a result, security breaches occur frequently and have become rampant, causing billions of dollars in loss each year since 2020. This has casted a dark cloud over efforts to leverage DeFi for financial inclusion, whether it is United Nations use of cryptocurrency fund for its various programs, or the play-to-earn DeFi games such as Axie Infinity that could help alleviate poverty in developing countries.

Security is the prerequisite of inclusiveness. Without security, the users of the DeFi system will suffer significant loss - in some cases, the lifetime losses. As such the mere access and use of the DeFi system does not necessarily provide financial inclusion for these users. On the contrary, the users could be further excluded from the financial system due to security breaches of the DeFi system.

In this paper, we discuss the DeFi security and regulatory issues such as price manipulation due to centralized oracles, weak key management practice, transaction spoof attacks, DNS attacks, access control attacks, front-running attacks and MEV, rug pulls, cross bridge attacks, regulatory uncertainty, lack of technology maturity, price volatility and poorly designed tokenomics.

As a prerequisite for making iDeFi systems more inclusive, we need to make them secure, e.g., by adopting the DevSecOps process in DeFi system development. In addition, we need to create awareness and educate people of security around the DeFi system. We also need to build capabilities for assessing the security of DeFi systems and issuing attestation and even certification. Finally, we need regulatory certainty around DeFi, balancing user privacy and the need for conducting KYC/AML checks.

1: Introduction

DeFi is a new vision of banking and financial services that is based on peer-to-peer payments through blockchain technologies. Via blockchain, DeFi allows “trust-less” banking, sidestepping traditional financial middlemen such as banks or brokers. Various financial transactions are possible with DeFi's 'smart contracts' that execute financial transactions under certain conditions. The users of DeFi do not need to register an account with the DeFi system. They only need to use a self-custodian wallet to get access to any DeFi system, thus increasing the security and portability[Werner et al, 2021].

In March, 2022, President Biden issued a much-anticipated executive order on cryptocurrency and digital assets, setting out key priorities and a roadmap. Among the key priorities, the executive order stated that “ Promote Equitable Access to Safe and Affordable Financial Services by affirming the critical need for safe, affordable, and accessible financial services as a U.S. national interest that must inform our approach to digital asset innovation, including disparate impact risk. Such safe access is especially important for communities that have long had insufficient access to financial services.” [The White House, 2021]

This order has a direct impact on the future of DeFi and especially lays out the high level requirements for equitable and secure access of DeFi applications. As one of Web3's top applications, DeFi has gained momentum during the global pandemic. DeFi has some advantages over traditional finance. In the next subsections, we will discuss the difference between DeFi and CeFi with examples, and also discuss some advantages of DeFi.

1.1: DeFi vs. or TradFi or CeFi

Traditional finance(TradFi) or centralized finance (CeFi) has been the cornerstone of modern capitalist society. In the TradFi system, intermediaries, like banks, stock exchanges, insurance companies play very central roles for financial transactions. And in order to complete transactions, all parties need to trust that those intermediaries will act fairly and honestly. In some literature [IvanOnTech, 2021, Shubham D., 2022], CeFi is defined differently from TradFi. CeFi is defined as organizations using crypto currency as one of main components in the system, but still leveraging traditional middlemen and also obtaining traditional license to operate in financial transactions. TradFi is completely disconnected from crypto currency, like some commercial banks without any crypto business. In our view both CeFi and TradFi are the same since they both need middlemen or intermediaries. As such, we use CeFi and TradFi interchangeably in this paper.

In DeFi , those intermediaries are replaced by smart contracts deployed on blockchain. Instead of transacting through intermediaries, people trade directly with one another, settling trades and ensuring that the entire process is fair and trustworthy.

Compared to CeFi, DeFi has many distinctive attributes and advantages, and as the technology continues to mature, its application range will become more extensive, and even bring about a revolution in the entire financial industry. Table1 has the high level comparison of CeFi vs. DeFi

Features	**CeFi/TradFi**	**DeFi**
KYC/AML verification	Yes	No
Custody	Yes	No
UI/UX	Friendly	Not Friendly
Intermediaries	Banks and Insurance	Smart Contracts
Governance	Traditional Corporate Structure	Decentralized Autonomous Organization

Table 1: Difference between CeFi and DeFi

The following table lists some examples of financial services offered by CeFi and DeFi.

Finance Service	**CeFi or TradFi**	**DeFi**
Centra Bank	Federal Reserve, PBOC	MakerDAO [MakerDAO, 2020] mStable[mStable, 2021], and most blockchain projects with ERC20 token issuance
Commercial Bank	Bank of America, HSBC	Compound[Leshner et al, 2019] AAVE[Aave, 2020] Venus [Venus, 2020]
Investment Bank	JP Morgan, Goldman Sachs	Centrifuge[Centrifuge, 2021]

		UMA[UMA 2018] MetaCartel[MCV, 2019]
Payment	PayPal, Apple Pay, Google Pay	BitCoin[Nakamoto, S., 2008] Ethereum[Buterin, V., 2014] And all other layer 1 public blockchains
Exchange	NASDEQ	Uniswap DyDX
Brokerage	Fidelity, Vanguard, ETrade	Primex.finance[Primex Finance, 2022]
Mutual Funds or ETF	Spider, Vanguard S&P 500 ETF (VOO)	Defi Pulse Index (DPI)[Schmidt, C., 2022]
Insurance	All State, State Farm	Nexus Mutual[Karp, H., etal., 2020] Opyn [Peaster, W., et al., 2022]
Global transaction settlement and clearing	SWIFT	Public blockchain and Smart contracts
Financial Infrastructure	Data Center or Cloud Services	Public blockchain, Web3 APIs, ENS, IPFS, RPC nodes, etc.

Table 2: Financial Server offered by CeFi and DeFi

1.2: The Benefit of Defi

In addition to increased security and portability from the user's perspective, DeFi has the following additional benefit.

Inclusiveness and equal access

DeFi is open and accessible via public blockchain. Anyone with internet access and blockchain wallet can have equal access to DeFi applications. Considering that more than 2 billion people worldwide still do not have a bank account (for example, the World Bank has stated that 60% of Latin American adults do not have an account at a financial institution [WorldBank Blogs, 2012]), providing DeFi service to the unbanked people worldwide will increase inclusiveness and reduce poverty.

Financial Sovereignty

One of DeFi's major advantages is that users always have absolute control or financial sovereignty over their assets[Werner, S.M. 2021].

Peer to Peer Service

With DeFi applications, users can play the role of customer or provider in financial transactions at will. The service provider does not need a bank or insurance license to operate, and the client does not need to go through a lengthy and expensive "Know your Customer" identity validation process. Users can be anywhere in the world with a blockchain wallet[Suratkar, S, 2020] and some digital assets fully under user's control to provide DeFi service or consume DeFi service[Schär, F., 2021].

Transparency

The DeFi protocol code is open source and running on a public blockchain, so anyone can verify its security, transaction rules, transaction histories, actual network usage, transaction volume, total locked value, and unique user address.

Censorship Resistance

Censorship resistance refers to the features of a network that prevent parties from altering or blocking data on it. Once the data is added, it should be virtually impossible to remove or alter it, making it permanent. In DeFi, the blockchain network nodes do not censor and alter individual transactions. Nevertheless, the network nodes can re-order the transaction and extract values from the re-ordering of the transaction. This problem is called "Miner extractable value" or "Maximum extractable value". We will revisit this issue later in this paper.

Programmability

DeFi is implemented through smart contracts, and smart contracts can be programmed and adjusted by the user community according to functional needs to align with different types of financial logic. The user community can be organized as an autonomous decentralized organization (DAO) to decide key parameters of financial logic.

Composability

This is also called “money lego”, meaning that the base level DeFi protocols implemented by smart contract can be leveraged by other DeFi projects to compose new DeFi applications. For example, DEX protocol UniSwap and DeFi lending protocol Compound can be leveraged by yield farm protocol to produce optimized yield by lending and swapping assets using these two protocols.

Zero Cost to have a DeFi Account

In traditional finance, in addition to transactional fees, there are often account fees. For example, the annual fee of a credit card or debit card or checking account (if the account does not meet minimum balance). In DeFi however, even if you only have zero balance of crypto assets in your account, you do not need to pay any account fees.

Regardless of the advantage listed above, the security and inclusiveness of DeFi systems are the top issues that need to be addressed. Indeed, DeFi’s recent access since pandemic has been mired with multi billions dollars loss due to smart contract security breaches. The lack of security was the main reason for slow adoption and reduced financial service inclusivity which can be offered by DeFi systems.

This paper analyzes some top DeFi security issues and countermeasures as well as suggesting key factors impacting inclusiveness of the DeFi system.

2: DeFi and Smart Contract Security issues

DeFi’s success has come at the expense of security issues, which need attention by all stakeholders in the ecosystem [Amler, H. et. al.,2021, CVE, 2022, CryptoSec, 2022, Wang, B. et. al., 2021 Buterin, V., 2016]. The following sections provide the list of most widely exploited security vulnerabilities in DeFi systems.

2.1 Price Manipulation due to Centralized Oracle data

Rather than using an external oracle, some poorly designed DeFi protocol frequently computes the value of the tokens they hold depending on a centralized price oracle. Flash loan assaults take advantage of this by dramatically manipulating a centralized price oracle [Yazdanparast, E., 2021, Wang, S.H. 2021, Synthetix, 2019]. This centralized price oracle causes the token's value to be calculated incorrectly, allowing the attacker to drain value from the DeFi system. Since 2021, this form of attack against DeFi protocols has become one of the most popular and devastating. BZX [BZX, 2021], Belt Finance[Halborn, 2021], and BurgerSwap[Behnke, R., 2021] are examples of protocols that have been exploited in this fashion. In order to defend against

this kind of attack, it is advised to use a decentralized oracle price feeder instead of using a centralized oracle price feed for the DeFi system.

2.2 Stolen and Leaked Private Keys

Blockchain technologies employ public key cryptography. The DeFi user uses a wallet application which stores private keys to sign the DeFi transactions. If the private key is stolen or leaked, then the crypto assets are lost[Winter, P.2021].

For example, in August, 2022, the Slope wallet was under attack due to its poor security design and coding that resulted in sending the user's private key and recovery words list (mnemonics) to a centralized logging server. The hacker was able to get access to the logging server and steal thousands of private keys. As such, about eight thousand Slope wallet accounts' private keys were lost and about $8 million in total of crypto assets were stolen[Hayward, A., 2022].

On March 29, 2022, Axie Infinity reported a loss of over $625 million USD caused by an attack on the Ronin network. The attacker used hacked private keys to steal funds in two transactions, one for 173,600 ether (ETH) and the other for 25.5 million USD Coin or USDS [Montaigne, B., 2022].

There are also phishing attacks on the private key: Hackers usually target developers or top executives from prominent DeFi protocols to phish for private keys. For example, in November, 2021, BZX protocol's developer's private key was stolen and $55 million lost. This attack granted the hacker access to the content of the bZx developers wallet, and also the private keys to the BSC and Polygon deployment of bZx Protocol [Avan-Nomayo, O., 2021]. For this kind of attack, it is easily avoided by separating the development duties from operation duties. The operation team should hold multiple signature keys and deploy protocol contracts using a locked down and safe workstation.

The following are effective countermeasures for private key breach:

- Don't Put all your tokens in one wallet. You should put the majority of tokens into a cold wallet that has no access to the internet. Only store a small amount of token with a warm wallet which has access to the internet.
- Use well-known wallet which has good and safe key generation and enough randomness
- Backup your wallets using cold storage or using paper wallet and store paper wallet into a safe. A paper wallet is just a paper with either recovery words (called mnemonics) or private key written.
- Beware of phishing scams. Do not click a link in email or download a file from an unknown party. Most wallet providers will not email or call their customer directly. If you have an issue with your wallet, use the wallet's provider's support website to open a

ticket. Never send your private key or mnemonics to a technical support person or any other person.

2.3 Spoof Transaction Attack

Spoof transaction attacks happen when the hacker was able to use a fake transaction to convince the user to approve or sign the transaction to steal funds with a hidden actual transaction. In this case, the private key is not stolen, the user was deceived with a fake transaction.

In December 2020, An attacker stole over $8 million worth of NXM tokens from Hugh Karp, the founder of DeFi insurer Nexus Mutual [Chipolina, S., 2021].

Nexus Mutual said that the attacker gained remote access to Karp's computer and modified the MetaMask extension on his browser. This enabled the attacker to create a spoof transaction that popped up while Karp was performing an unrelated action in MetaMask. "I subsequently approved it, thinking it was the transaction I was intending to conduct. Instead, it was transferring NXM to their wallet," he explained. Karp added that his private keys are still secure, as the hacker didn't manage to access them.

To prevent spoof transaction attacks, one needs to be very careful and verify that the wallet used is a genuine wallet, and inspect the transactions before signing it.

The user also needs to be aware of clickjacking attacks. Clickjacking is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. Its other name, user interface (UI) redressing, better describes what is going on. Users think they are using a web page's normal UI, but in fact there is a hidden UI in control; in other words, the UI has been redressed. When users click something they think is safe, the hidden UI performs a different action. Clickjacking itself is not the end goal of the attack; it is simply a means of launching some other attack by making users think they are doing something safe. The actual attack can be virtually anything possible via web pages, including a web page with the link to a malicious smart contract or promoting users to enter seed phase to their wallets or installing malicious wallet extensions, etc.

2.4 Domain Name Service (DNS) hijacking attack

DNS is used by most Web2 and Web3 applications to resolve the domain name to the actual IP address. This allows users to access websites via simple text-based web addresses instead of typing out the exact IP address of each website they wish to visit, making the web easier to use. If the hacker was able to hijack the DNS, the hacker can post fake smart contract links to deceive the user to deposit the funds to a fake smart contract and then the hacker can drain the

funds from the fake smart contract. Or the fake website will just steal user seed phrase, private key and numonics.

In March 2021, both Cream Finance and PancakeSwap reported that DNS spoofers had compromised their websites[Foxley, W. 2021]. The attack resulted in both DeFi protocols' front-end websites requesting users to enter their seed phrase. If entered, the phrase would allow the attacker to take control of users' wallets and drain their funds.

In June 2022, Convex Finance, a protocol offering boosted rewards for Curve liquidity providers and stakers, confirmed that its website's DNS was hijacked.The hacker posted a link to the malicious smart contract that can steal users' funds[McSweeney, M., 2022].

To counter this kind of attack as web3 users, we need to carefully verify the addresses involved in every single crypto transaction.Even if you trust the website, you need to verify if the smart contract posted in the trusted website is genuine. You can see the transaction history of the site, and if there are very few transactions, this could be a malicious smart contract. Even if there are many transactions with the smart contract, you may still want to send small funds to test. You should not approve an infinitive amount of funds.

As web3 developers, we can use Domain Name System Security Extensions (DNSSEC) to add cryptographic authentication and defend against spoofing attacks[Eastlake, D.E., & Kaufman, C. 1997].

2.5 Access Control Attacks

Access is usually controlled by indicating that calls to a function must be made by one or more addresses from a list of addresses. These access controls are sometimes omitted or built in a way that allows an attacker to circumvent them. If this happens, the attacker gains privileged access to the contract, allowing them to extract value from it.

In August 2021, the Poly Network($610 million stolen [Mitchell Clark. 2021]) and Punk Protocol (8.9 million stolen[Rob Behnke, 2021]) were hacked. In both cases, the attacker claimed ownership over the projects' contracts and utilized that access to drain value from them.

The countermeasure is to define access control policy for your smart contract and to make sure there is separation of duty and least privilege access control policy based on business and security requirements. For example, the owner or deployer of the smart contracts should not have all privileges as this will be a centralization risk and if the hacker steals the contract owner's private key, there will be no recourse to save the DeFi project. Instead, leveraging DAO and voting mechanisms for some of the important access control privileges. Leveraging multisig or multipart computation for private key material storage and sharing is also a good practice.

In addition, DeFi projects shall use third party audits of smart contracts and bug bounty programs such as Immunify (https://immunefi.com/) to offer rewards to whitehat security researchers to find security bugs and fix them before launching your DeFi project.

2.6 Frontrunning Attacks and general MEV attacks

Blockchains do not immediately add transactions to the distributed ledger. Transactions are broadcasted to the blockchain network as soon as they are created but are stored in mempools on each blockchain node until they are added to the ledger as part of a block.

The gap between the creation of a transaction and its inclusion in the ledger creates the opportunity for frontrunning attacks. The attacker (commonly a bot, a searcher, or a miner) will look for transactions that they can exploit (taking advantage of Maximum Extractable Value or MEV). If they see one, they create their own version of the transaction with a higher transaction fee and transmit it to the network. Since blockchain miners commonly order transactions in blocks based on their transaction fee, the attacker's transaction comes before the original one, netting them a profit [Daian, P, 2020].

Frontrunning impacts DeFi security in a few ways. Many bots will use frontrunning to make a profit based on foreknowledge of users' transactions[A. Judmayer. etal., 2020; M. Kelkar et al, 2020]. In some cases, this is malicious. in others (such as the DODO DEX and Punk Protocol hacks), a bot frontruns an attempted exploit and then returns the stolen tokens to the exploited protocol.

Currently, there are no effective security measures for front running. There is some research on using flashbot to democratize the front running and MEV opportunity (https://docs.flashbots.net/).

Ethereum core developers are doing research on separation of block proposer and block validator to reduce and mitigate the risk of front running and MEV. Other researches include using private transactions, secure multiplat computation, and directed acyclic diagram for MEV attack mitigation[Hunag, K., 2022].

2.7 Rug Pulls

Many attacks on DeFi protocols come from external threats, but this is not always true. In some cases, DeFi users are the victims of attacks from the developers and owners of the protocol itself.

Rug pulls and Ponzi Schemes are attacks committed by the owners and developers of the DeFi protocols. In a rug pull scheme, someone inside the company with privileged access to its contracts uses this access to drain funds from the protocol. Typically, the project and the team behind it then disappear, leaving the victims with little recourse to address the issue.

One of the Chainalysis blog post notes[Chainanalysis, 2021], “Rug pulls have emerged as the go-to scam of the DeFi ecosystem, accounting for 37% of all cryptocurrency scam revenue in 2021, versus just 1% in 2020.” The Chainalysis blog post also provides examples of some of the biggest rug pulls of 2021. For instance, the AnubisDAO case is mentioned as the second-biggest rug pull of this year, with over $58 million worth of cryptocurrency stolen.

According to the post, AnubisDAO launched on Oct. 28, 2021, with claims of offering a decentralized currency backed by a number of assets. However, the project didn’t contain a website or white paper, and all of the developers went by pseudonyms. Miraculously,

AnubisDAO still managed to raise nearly $60 million overnight[Hakki, 2021], yet 20 hours later, all of those funds disappeared from AnubisDAO’s liquidity pool.

It is important for DeFi users to do due diligence before investing or transacting on a DeFi project. Usually, an anonymous team is a red flag. If the smart contract is not audited, it is yet another flag. If the price of the project token pumps a lot recently, then it is yet another red flag. It is wise to be patient and wait to see instead of falling into the FOMO (Fear of Missing Out) trap.

2.8 DeFi Cross Chain Bridge Attack

DeFi Bridges are frequently targeted because they provide a centralized source of funds for the ‘bridged’ assets on the receiving blockchain. According to some experts, efficient bridge architecture is still in its early stages. Furthermore, some developers’ awareness of security procedures is still somewhat limited, leaving their systems vulnerable to a hacker attack.

According to a report published by ChainAnalysis on August 2, 2022, 69% of Stolen Tokens or about $2 billions from January to August 2022 was from Cross-Chain Bridge[Economictimes. 2022].

The following is some effective defense measures to counter the bridge attacks for DeFi developers:

- Whenever possible, understand the risk associated with bridging and avoid bridging for users without their consent.
- Check whether the assets in the bridge are insured, and if not, whether insurance could be set up for them.
- Avoid infinite approvals when interacting with external protocols—only approve the amount that you absolutely need during the interaction.
- And always make sure the bridge contracts are fully audited by multiple independent security firms.

For users:

- Only use bridges that have been audited by several highly reputable security firms.
- Check the audit reports to see if issues that were found have actually been fixed, not simply acknowledged. If you aren't familiar with how to interpret audit results, check out one of our recent posts explaining how to read an audit report.
- Check whether the bridge has a bug bounty program in place. Bounty programs incentivize white hat hackers to review the code and disclose vulnerabilities before they are exploited by bad actors.

While bridges present numerous risks and vulnerabilities, the demand to transfer assets from one blockchain to another is not going away. Bridges give end users access to a diverse range of DeFi protocols, and allow developers to easily launch dapps across multiple blockchains. Following a surge of growth at the end of 2021, it is likely this trend will continue. However, as more cross-chain bridges launch, exploits will also continue to occur. By being aware of the risks involved and employing the best practices outlined above, both bridge users and blockchain developers can hopefully experience more of the benefits of bridging assets while avoiding some of the pitfalls.

2.9 Other Top Smart Contract Vulnerabilities

The following table summarizes the top smart contract programming vulnerabilities and the real world hacks and associated loss of funds in USD.

Vulnerability Name	**Vulnerability Description**	**DeFi project attacked**	**Date**	**Loss Amount (million USD)**
Arithmetic Vulnerability	Vulnerabilities due to arithmetic underflow or overflow[Torres, C. et.al. 2018]	Uranium Finance Compound Pizza DeFi Umbrella Network	April 2020 September 2021 December 2021 March 2022	50 80 5 0.7
Reentrancy Vulnerability	A reentrancy attack occurs when a function makes an external call to another untrusted contract. Then the untrusted contract makes a recursive call back to the original function in an attempt to drain funds[Xue, Y. 2020]	dForce Akropolis Grim Finance	April 2020 November 2020 December 2021	24 2 30

Logical Vulnerability	These vulnerabilities can be due to typographical errors, misinterpretation of specifications, or more serious programming errors. Logical errors tend to be related to the security and functionality of smart contracts.	bZx BurgerSwap Eleven Finance Punk Protocol Starstream Finance	November 2020 May 2021 June 2021 August 2021 April 2022	8 7 4 3 4

Table3: Smart Contract Programming Vulnerabilities Hacks and Loss of Funds in USD

2.10 Other DeFi Security Risks

Other risks of DeFi ranges from Regulatory uncertainty to financial models and are briefly discussed below:

Regulatory Uncertainty

Crypto and DeFi are undergoing rapid innovation and are global in nature. But these global DeFi organizations must still engage in international transactions and meet local regulatory requirements or risk the potential for foreign sanctions. DeFi's regulatory environment is still highly uncertain, and it remains to be seen how regulators in the U.S. or other countries will enact policies affecting the ecosystem.

For example, should certain DeFi tokens be deemed securities? If so, it would likely hamper their liquidity and harm adoption and the speed of innovation. Should certain stablecoins become more heavily regulated, they could be forced off DeFi platforms, which would harm DeFi services that rely on these fiat-backed assets as collateral.

Due to the recent demise of Luna's UST stablecoin. The regulation on stablecoin by the United Statement and European Union is upcoming.

On August 8, 2020 the tumbler/mixer Tornado Cash was sanctioned by the Office of Foreign Assets Control (OFAC), an enforcement agency within the U.S. Department of the Treasury. According to a press release from the U.S. Treasury, Tornado Cash had been used to launder more than $7 billion worth of virtual currency since its founding in 2019, including more than $455 million stolen by the Lazarus Group, a cyberterrorism group sponsored by the North Korean government.

The specific action taken by OFAC was to add Tornado Cash to its Specially Designated Nationals (SDN) blacklist, which effectively removes the entity from the global financial system and explicitly bans "U.S. persons", including digital asset exchanges operating in the U.S., from transacting with it. This is a novel action: for the first time, the U.S. The Department of the Treasury has sanctioned a smart contract and a tool. The outcry[Tapscott., A., 2022] for this the crypto community is also loud and many believe that open source smart contracts are under the protection of the First Amendment[Inside, 2022].

Few days after OFAC's sanction, on August 10, 2022, the Dutch Fiscal Information and Investigation Service (FIOD) said it arrested a 29-year-old man in Amsterdam who is one of the developers of Tornado Cash[Coindesk, 2022]. The unnamed individual is suspected of "involvement in concealing criminal financial flows" and "facilitating money laundering through the mixing of cryptocurrencies" using Tornado Cash.

"Multiple arrests are not ruled out," FIOD wrote on its website. "Also in the cryptocurrency domain, the FIOD stands for a safe financial Netherlands and investigates with effect and impact. Today the suspect is brought before the examining judge."

DeFi will be certainly impacted by more upcoming regulations and/or enforcement by authorities in different countries. The incorporation of futures regulations into DeFi are still playing out. A good balance of regulation and innovation with particular focus on security and inclusiveness will be a sensible approach.

The DeFi community needs to educate lawmakers on how technologies work and provide them with a longer-term and broad view of the different components in the ecosystem. It is also important for DeFi developers to keep abreast of the new regulation and develop DeFi protocol which is in full compliance with the local regulations.

Tech Maturity

Crypto networks and DeFi technology are still nascent and continue to mature. There are many areas where the technology may still need to improve before DeFi can service a more sizable global financial market. Some of these areas include underlying blockchain network scalability, smart contract security, DeFi technical architecture and UX/UI design, among other areas.

Crypto Asset Price Volatility

Crypto assets prices have been subject to high volatility. Negative fluctuations in the value of a DeFi protocols' crypto holdings may materially harm the dApps usage, DeFi revenue, user community, user participation, and, ultimately, the risk of some DeFi applications.
The price volatility in some cases are associated with the pump and dump scheme that either the DeFi project developers or investors or some insiders conduct to profit from regular DeFi users. As DeFi users, if one observes that some DeFi token price jumped very high for no reason or a reason that is too good to be true, it usually indicates a pump-and-dump scheme. The best protection is to stay away from these kinds of DeFi projects and their tokens [Ferber, L,. 2022].

DeFi Tokenomics and Financial Models

Many DeFi projects use governance tokens affiliated with the protocol. However, it's yet to be fully seen how many of these digital assets will accrue long run sustainable value tied to the

fundamental growth of the dApp. Some token models have proved to be a failure. For example, the Luna and Terra USD token model for stablecoin has encountered a death spiral during the year 2022 crypto winter[Rai, R. 2022].

3: Towards secure and inclusive DeFi system

As of time of this writing (August 2022), DeFi is too technical, too volatile and too "geeky" for most people to understand and use. The following conditions will have to be met in order for DeFi to provide equal and safe access to global users, especially to those billions of people who are unbanked.

3.1 Improve DeFi Smart Contract Security

As discussed previously in this paper, DeFi security risks are largely due to smart contract security holes. It is important to get smart contracts audited by a few independent smart contract audit firms before contracts are deployed to the mainnet. In addition to security audits of smart contracts, it is important for the project team to adopt the DevSecOps process which defines the security at the early stage of development and continuously integrate security controls during the development, deployment and operation stages of DeFi protocol.
DeFi developers can use formal verification and other security tools to validate security of smart contracts [Nam, W., Kil, H., 2022, Nguyen, T. et. al., 2021],

3. 2 Education and awareness

Due to the complex and composable logic of DeFi protocol, it is hard for everyday Joe to understand the intricacy of the DeFi and as such the benefits of DeFi largely are reaped by early adopters who have background in either finance or programming or both. Education and awareness training is necessary for mainstream users to understand the benefits and pitfalls of DeFi. It is also very important to educate the regulators and policy makers about DeFi so a balanced and clear regulation can be enacted to promote the healthy growth of the industry.

UniSwap's "DeFi Education Fund," is a good example of such efforts[Uniswap DAO, 2021]. The Fund is a 501(c)(4) nonprofit entity based in the United States to provide grants for political, educational, and legal engagement. The 501(c)(4) will fund education and advocacy through both existing advocacy organizations and potentially new ones. The funding will have the goals of 1) challenging misguided regulatory, legal, and political threats to decentralized finance; 2) achieving regulatory clarity for decentralized finance and related activity; 3) advancing laws that support decentralized finance and decentralized governance; and 4) spurring other DeFi protocols' governance bodies to contribute to the effort (through this entity or their own). The entity is nonpartisan and global in approach and orientation.

Some other initiatives in DeFi education and advocacy are provided by organizations such as Coin Center, Fight for the Future, the Blockchain Association, the Crypto Council for Innovation, the Defi Alliance, and Blockchain for Europe.

3.3 Scalable base blockchain

One of the main obstacles to mainstream adoption of DeFi is the scalability of the base blockchain. The cost to engage in DeFi transactions in Ethereum is very expensive (could be multiple hundred of dollars for lending your token or borrowing tokens) and the transaction per second is slow at average 15 per second. There are many scalability solutions as discussed in many literature. The most promising is the layer 2 protocol such as rollup protocol on ethereum or some other layer 1 approach such as Binance Smart Chain, Solona, or Aptos.

The cross chain solutions such as Polkadot and Cosmos also are attractive for DeFi protocol developers to bridge different DeFi protocols to develop new DeFi systems. It is important to note that there is a trilemma which states that it is impossible to achieve securive, scalility and decentralization at the same time. One can only meet two of the three requirements at the same time[Buterin, V., 2021]. For example, you have to sacrifice the decentralization if you need to meet security and scalability requirements. Or you have to compromise with scalability if you want to meet the requirements of security and decentralization. The Ethereum base chain[Buterin, V., 2014] has strong security and decentralization and this comes at the expense of scalability. All layer2 solutions or other layer 1 alternatives to ethereum have been able to achieve good scalability with the expense of decentralization.

3.4 Global Reach

DeFi is usually operated on public and permissionless blockchains and by its nature is boardless. The global reach from a pure technology perspective is given for users who can use VPN to bypass some of the local restrictions.

From the community development and ecosystem perspective, the global reach is not easy and largely depends on how DeFi builders reach out to the global community. Many well known KOL and crypto media companies played crucial roles to educate and help project teams to reach out to global users.

3.5 UI/UX Design

Most DeFi applications developed so far have very poor UI/UX design. UI (User Interface) and UX (User Experience) are terms that mean very different things, but only together can they help create a user-friendly DeFi product for mainstream adoption. If you want your DeFi products to stand out from the crowd and conquer the market, you need an innovative UX/UI design.

But it is important to understand the difference between the two terms. UI is directly related to how to present your product, and UX as to how it works, the interaction between the app and the user. Both are mandatory in the process of creating a product, but UI is only a small fraction of the ecosystem that generates and influences the UX of a product.

UI Design involves managing and manipulating various forms of content (text, images, graphics, video), fields, and functions (buttons, labels, boxes, commands, drop-down lists) but also action items (what happens when you click on). It requires a touch of art and emphasizes emotion, and the goal is to create a clean and beautiful interface that will make the DeFi product very attractive to users.

UX Design has a much wider spectrum and includes several elements (architecture, interaction, content, user research) which together highlight the product's ability to meet the needs of DeFi users.

3.6 CeFi's participation in DeFi.

For DeFi to be adopted by mainstream investors, CeFi's participation will be very important. Indeed, the traditional financial institutions such as Fidelity, JP Morgan and even Goldman Sachs have been trying to offer some degree of DeFi services to its customers.
Since October, 2018, Fidelity Digital Asset Services has started to provide custody for cryptocurrencies such as bitcoin and to execute trades on multiple exchanges for investors such as hedge funds and family offices. Fidelity CEO Abby Johnson called the company's crypto custody business "incredibly successful." Johnson reiterated Fidelity's focus on connecting the industry of crypto-assets with traditional financial sectors[Michael Lavere 2020].

In July, 2021, Global investment bank JPMorgan has reportedly green-lighted its advisors to provide clients with access to five cryptocurrency funds. The funds are available to all JPMorgan's wealth management clients seeking investment advice. JPMorgan told its advisors that effective July 19, 2021, they can take orders to buy and sell five cryptocurrency products [Kevin, H., 2021].

Four of them are from Grayscale Investments: the Bitcoin Trust, Bitcoin Cash Trust, Ethereum Trust, and Ethereum Classic Trust. The fifth approved fund is Osprey Funds' Bitcoin Trust.
A person directly familiar with the move said that the new offering applies to all JPMorgan clients seeking investment advice, including the bank's self-directed clients using its commission-free Chase trading app, mass affluent clients whose assets are managed by financial advisors under JPMorgan Advisors, and ultrarich clients serviced by the firm's private bank. These five funds can be viewed as a bridge to DeFi funds although they are not DeFi funds.

In an interview with Bloomberg in November, 2021, Damian Courvalin, Head of Energy Research at Goldman Sachs, talked about the outlook for gold and crypto: "Just like we argue that silver is the poor man's gold, gold is maybe becoming the poor man's crypto." He sees

funds starting to flow from gold into bitcoin as inflation fears escalate, noting that “We’ve argued historically that crypto and gold do not have to cannibalize each other.” Courvalin continued: “At this point, there may be enough wealth to allocate to both, especially, I think, as that inflation signal is starting to be more pressing.” He further noted: “The value of crypto is its network, just like the value of oil is the fact that it’s consumed. Gold, like diamonds and art, doesn’t have that. It’s just a pure defensive asset that can outperform over a significant period of time.”

The Goldman Sachs DeFi ETF funds filed with SEC in July 2021 provides investors with exposure to companies aligned with the themes of blockchain technology and the "digitalization of finance," says the bank. Since there are no actual DeFi companies and stocks included in Goldman Sachs’s DeFi ETF, the crypto community criticized the move. One tweet by @CharlieShrem noted that: “Goldman Sachs’s “DeFi” Fund contains only legacy companies and has 0 crypto-native companies. They’re trying to deceive the public into thinking we already have decentralized finance. Fix the money, fix the world”.

3.7 Regulatory Certainty

Although the absence of regulation might be one of the attractive aspects of DeFi for some users and developers, there is a desire in the industry for regulatory certainty, and any announcement on decentralized finance from a regulatory body signals its legitimacy as an alternative to traditional finance. For an industry to thrive, regulation certainly is necessary in the long run.

Unfortunately, there is no comprehensive regulation available in any county.

The recently enacted infrastructure bill in November 2021 includes an ad hoc regulation targeting the tax reporting requirements. It brings more questions and clouds to DeFi than to providing any clarity. The amadament in the infrastructure bill stipulated the IRS reporting requirements that make it necessary for businesses to share details about senders of digital assets. It’s an amendment to tax code section 60501.

This law is designed to target criminal activities. The reporting burdens will not only apply to intermediaries (exchanges, etc.) but will apply to all businesses and could potentially include individuals. The only businesses which are exempt are banks and financial institutions which already report such information under the Bank Secrecy Act. It defines cash to include “any digital asset,” so all digital currencies, NFTs, and other digital items are covered. As with all laws, and especially when they apply to new technology, there will be various interpretations and disputes about when the law applies and to whom.

Due to the peer to peer nature of the DeFi business, each DeFi user can be both the customer and provider of the DeFi business. So, it is very hard to implement the amadenmant in reality.

For example, If an individual provides liquidity to a DeFi exchange pair pool and then cashes out by withdrawing their liquidity, how will it be possible for a DeFi protocol developer to know who exactly the liquidity providers are? If a user leverages DeFi to lend or borrow crypto currency using a self sovereign wallet via smart contract, how can the DeFi lending protocol know the user's actual identity? If DeFi platforms do not know the user's actual identity, how can they provide accurate reporting? If a user stakes a DeFi token via a smart contract and gets the rewards for staking and protecting the security of the DeFi platform or the base blockchain, how can the anonymous nature of staking be reconciled with the reporting requirements? There are so many unanswered questions to this amendment in the infrastructure bill.

3.8 KYC/AML

Regarding how to use DeFi to perform KYC, we can take some lessons learned from some of the ideas of digital yuan developed in China. Digital yuan allows the smart amount to be transferred between peers without KYC/AML. Only a large amount of funds transfer requires KYC/AML.

Another solution is to leverage Decentralized DIdentity (DID) standard and Verifiable Claim standards currently under heavy development at W3C and Decentralized Identity foundation. As the DID standard and implementation of it become mature, we can see that KYC/AML can be applied to DeFi protocols which allow the DeFi protocol to be integrated with Verifiable Credential providers to get the KYC/AML services needed for some transactions while simultaneously protect user's anonymity and privacy using zero knowledge proof.

During the Bankless interview in November 2021, CFTC former chairman Chris Giancarlo (Crytpo Daddy) suggested that the regulations for DeFi should not force every regular user to go through the traditionally KYC/AML process. Instead, DeFi ecosystems should use big data and AI to track terrorist and monery laudering activiteis. He suggested that the activity based monitoring and surveillance based on bid data analysis is a much better approach than traditional identity based monitoring and surveillance. He further argued that the regulators should look at innovation which can benefit society changes instead of innovation which is only good within the existing regulatory framework[Bankless, 2021].

4: Summary

In this paper, we discussed security as a precondition for nclusive DeFi systems. Although the whole DeFi industry is still in its first innings towards a scalable, global, secure and inclusive financial industry, there have been many successes since 2020.

The initial success of DeFi is mired with security breaches that cost billions of dollars due to the lack of security measures in the implementation and deployment process. We have listed some common DeFi security issues and potential countermeasures. We have also discussed what will be needed in order to build a secure and inclusive DeFi system.

More work will be needed as the DeFi system evolves and new business models and tokenomics gain momentum. DeFi is an innovation in the cross section of technology, finance, economics and game theory.

As security is a prerequisite for inclusiveness of DeFi systems, the security practice in the areas of smart contract security, wallet security, key management, access control, and the adoption of DevSecOps will also gain attention and investment from industry participants due to past and future security breaches.

5: Reference

1. AAVE, 2020. Aave Protocol Version 1.0. URL: https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf [Accessed 7 July, 2022]
2. Adams, H., Zinsmeister, N., Salem, M., Keefer, R., Robinson, D., 2021. Uniswap v3 core. URL: https://uniswap.org/whitepaper-v3.pdf. (ac- cessed 24 July 2022).
3. Amler, H., Eckey, L., Faust, S., Kaiser, M., Sandner, P., Schlosser, B., 2021. Defining defi: Challenges & pathway, in: Proceedings of the 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 181– 184.
4. Angeris, G., Chitra, T., 2020. Improved price oracles: Constant function market makers, in: Proceedings of the 2nd ACM Conference on Ad- vances in Financial Technologies (AFT), pp. 80–91.
5. Avan-Nomayo, O., 2021. DeFi protocol bZx compromised again: $55 million stolen in private key leak. URL: https://www.theblock.co/linked/123429/defi-protocol-bzx-compromised-again-55-million-stolen-in-private-key-leak [Accessed 18 August, 2022]
6. BadgerDAO, O., 2021. Badgerdao exploit technical post mortem. URL: https://badger.com/technical-post-mortem. (accessed 24 July 2022).
7. Bankless, 2021. The Fight for the Future of Money | CryptoDad Chris Giancarlo. URL: https://www.youtube.com/watch?v=NeQrSWa_qy8 [Accessed 30 July 2022]
8. Bartoletti, M., Chiang, J.H.y., Lafuente, A.L., 2021. Towards a theory of decentralized finance, in: Proceedings of the International Conference on Financial Cryptography and Data Security (FC), pp. 227–232.
9. Behnke, R., 2021. Explained: the Burgerswap Hack. URL: https://halborn.com/explained-the-burgerswap-hack-may-2021. [Accessed 18 August, 2022]
10. Buterin, V., 2016. Critical update re: Dao vulnerability. URL: https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulne rability/. (accessed 3 August 2022).
11. Buterin, V., 2014. Ethereum White paper. URL: https://ethereum.org/en/whitepaper/ [Accessed 8 August, 2022]
12. Buterin, V., 2021. Why sharding is great: demystifying the technical properties. URL: https://vitalik.ca/general/2021/04/07/sharding.html

13. bZx Contributor, 2021. Preliminary post mortem. URL:https://bzx.network/blog/preliminary-post-mortem. (accessed 26 July 2022).
14. Centrifuge, 2021. https://docs.centrifuge.io/ [Accessed 8 August, 2022]
15. Chainanalysis. 2021. The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Cryptocurrency Scam Revenue Close to All-time Highs URL: https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/ [Accessed July 8, 2022]
16. Chipolina, S., 2021. Here's What Happened to Nexus Mutual CEO's Stolen Funds. URL: https://decrypt.co/51536/heres-what-happened-to-nexus-mutual-ceos-stolen-funds [Accessed 18 August, 2022]
17. Coindesk, 2022. Netherlands Arrests Suspected Developer of Sanctioned Crypto-Mixing Service Tornado Cash. URL: https://www.coindesk.com/policy/2022/08/12/netherlands-arrests-suspected-tornado-cash-developer [Accessed August 20, 2022]
18. CryptoSec, 2022. Documented timeline of defi exploits. URL: https://cryptosec.info/defi-hacks/. (accessed 27 July 2022).
19. CVE, 2022. Cve search results. URL:https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=smart+contract. (accessed 21 July 2022).
20. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breiden- bach, L., Juels, A., 2020. Flash boys 2.0: Frontrunning in decentral- ized exchanges, miner extractable value, and consensus instability, in: Proceedings of the IEEE Symposium on Security and Privacy (SP), pp. 910–927.
21. Eastlake, D.E., & Kaufman, C. 1997. Domain Name System Security Extensions. RFC, 2535, 1-47.
22. Economictimes. 2022. Crypto worth $2 billion stolen from cross-chain bridges in 2022. URL: https://economictimes.indiatimes.com/news/international/uk/chain-analysis-2-billion-worth-of-crypto-stolen-from-cross-chain-bridges-in-2022 [Accessed August 19, 2022]
23. Ferber, L,. 2022. How Crypto Investors Can Avoid the Scam That Captured $2.8 Billion in 2021. URL: https://time.com/nextadvisor/investing/cryptocurrency/protect-yourself-from-crypto-pump-and-dump [Access 18 August 2022]
24. Foxley, W. 2021. DeFi Projects Cream Finance, PancakeSwap Hit With 'DNS Hijacks'. URL: https://www.coindesk.com/tech/2021/03/15/defi-projects-cream-finance-pancakeswap-hit-with-dns-hijacks [Accessed 18 August, 2022]
25. Hakki., T. 2021. AnubisDAO Investors Lose $60 Million in Alleged Rug Pull. URL:rypt.co/84924/anubisdao-investors-lose-60-million-in-alleged-rug-pull [Accessed July 8, 2022]
26. Halborn, 2021. Explained: the Belt Finance Hack. URL: https://halborn.com/explained-the-belt-finance-hack-may-2021/
27. Hayward, A., 2022. Solana Hack Blamed on Slope Mobile Wallet Exploit. URL: https://decrypt.co/106680/solana-hack-blamed-slope-mobile-wallet-exploit. [Accessed 18 August, 2022]

28. Huang, Ken, et. al 2022. Sok: On the Analysis of MEV Attacks and Defense, Blockchain Security Working Group white paper, Cloud Security Alliance, GCR.
29. Inside. 2022. Tornado Cash sanctions violate 'freedom of speech' protected by First Amendment, says CEO of Kraken. URL: https://inside.com/cryptocurrency/posts/tornado-cash-sanctions-violate-freedom-of-speech-protected-by-first-amendment-says-ceo-of-kraken-305210. [Accessed 20 August, 2022]
30. IvanOnTech, 2021.Making Sense of Traditional Finance and CeFi vs DeFi. URL: https://academy.moralis.io/blog/making-sense-of-traditional-finance-and-cefi-vs-defi [accessed on 22 March, 2022]
31. Juliano, A., 2018. dYdX: A Standard for Decentralized Margin Trading and Derivatives. URL: https://whitepaper.dydx.exchange [Accessed 8 August, 2022]
32. Karp, H., Melbrardis, R., 2020. NEXUS MUTUAL: A peer-to-peer discretionary mutual on the Ethereum blockchain URL: https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.p [Accessed 8 August, 2022]
33. Kevin, H., 2021. JPMorgan Begins Offering 5 Cryptocurrency Funds to Clients. URL: https://news.bitcoin.com/jpmorgan-begins-offering-5-cryptocurrency-funds. [Accessed 30 July, 2022]
34. "Leshner, R., Hayes, G., 2019. Compound: The Money Market Protocol. URL: https://compound.finance/documents/Compound.Whitepaper.pdf [Accessed 7 July, 2022]
35. M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels. 2020. Order-fairness for byzantine consensus. In D. Micciancio and T. Ristenpart, editors, Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III, volume 12172 of Lecture Notes in Computer Science, pages 451–480. Springer
36. MakerDAO, 2020. The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. URL: https://makerdao.com/en/whitepaper [Accessed 16, March, 2021]
37. McSweeney, M., 2022. Curve staking platform Convex suffers DNS hijacking. URL: https://www.theblock.co/linked/153964/curve-staking-platform-convex-announces-website-dns-hijacking [Accessed 17, August, 2022]
38. MCV, 2019, MetaCartel Ventures White paper. https://github.com/metacartel/MCV/blob/master/Whitepaper.pdf [Accessed 8 August, 2022]
39. Michael Lavere 2020. Fidelity CEO Says Firm’s Bitcoin Custody Business is ‘Incredibly Successful’. URL: https://www.cryptoglobe.com/latest/2020/12/fidelity-ceo-says-firms-bitcoin-custody-business-is-incredibly-successful [Accessed 30 July, 2021]
40. Mitchell Clark. 2021. Poly Network hacker gave back more than $600 million in stolen crypto. URL: https://www.theverge.com/2021/8/23/22638087/poly-network-600-million-stolen-crypto-hack-restored-defi [Accessed 17 August, 2022]
41. Montaigne, B., 2022. DeFi’s Largest Attack: What Happened to Axie Infinity’s Ronin Network. URL:

https://taxbit.com/blog/defis-largest-attack-what-happened-to-axie-infinitys-ronin-network [Accessed 18 August, 2022]
42. mStable, 2021. What is mStable? URL: https://docs.mstable.org/#what-is-mstable [Accessed on 22 March, 2022]
43. Primex Finance, 2022. Primex Finance Litepaper. URL: https://primex.finance/ [Accessed 8 August, 2022]
44. Rai, R. 2022. The Death Spiral: How Terra's Algorithmic Stablecoin Came Crashing Down. URL: https://www.forbes.com/sites/rahulrai/2022/05/17/the-death-spiral-how-terras-algorithmic-stablecoin-came-crashing-down [Accessed 17 August, 2022]
45. Reynolds, K., Kessler, S., 2022. DeFi Lender Rari Capital/Fei Loses $80M in Hack. URL: https://www.coindesk.com/business/2022/04/30/defi-lender-rari-capitalfei-loses-80m-in-hack/ [Accessed 18 August, 2022]
46. Rob Behnke, 2021. Explained: the Punk Protocol Hack. URL: https://halborn.com/explained-the-punk-protocol-hack-august-2021/ [Accessed 19 August, 2022]
47. Schär, F., 2021. Decentralized finance: On blockchain-and smart contract- based financial markets. FRB of St. Louis Review doi:http://dx.doi.o
48. Schmidt, C., 2022 Introducing The DeFi Pulse Index. URL: https://www.defipulse.com/blog/defi-pulse-index [Accessed 8 August, 2022]
49. Shubham Dhage, 2022. DeFi, CeFi, or TradFi: How will the future economy be? URL: https://www.soluntech.com/blog/defi-cefi-or-tradfi-how-will-the-future-economy-be. [Accessed 8 August, 2022]
50. Suratkar, S., Shirole, M., Bhirud, S., 2020. Cryptocurrency wallet: A review, in: Proceedings of the 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), pp. 1–7.
51. Synthetix, 2019. Synthetix response to oracle incident. URL:https://blog .synthetix.io/response-to-oracle-incident/. (accessed 21 June 2022).
52. Tapscott., A., 2022. The recent crackdown on Tornado Cash sets a dangerous precedent. Here's why it could be the beginning of an all-out 'war on code'. URL: https://fortune.com/2022/08/19/crackdown-tornado-cash-dangerous-precedent-tech-war-on-code-privacy-crypto-regulation-alex-tapscott [Accessed 19 Auhust, 2022]
53. The White House, 2021. Executive Order on Ensuring Responsible Development of Digital Assets. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets. [accessed on 22 April, 2022]
54. Torres, C.F., Schütte, J., State, R., 2018. Osiris: Hunting for integer bugs in ethereum smart contracts, in: Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC), pp. 664–676.
55. UMA, 2018. UMA: A Decentralized Financial Contract Platform. URL: https://umaproject.org/UMA-whitepaper.pdf [Accessed 8 August, 2022]
56. Uniswap DAO, 2021. Uniswap Education Funds Proposal. URL: https://gov.uniswap.org/t/governance-proposal-005-defi-education-fund/12963 [Accessed June 30, 2021]

57. Venus, 2020, Venus: The Money Market & Synthetic Stablecoin Protocol. URL: https://venus.io/Whitepaper.pdf [Accessed 7 July 2022]
58. Wang, B., Liu, H., Liu, C., Yang, Z., Ren, Q., Zheng, H., Lei, H., 2021. Blockeye: Hunting for defi attacks on blockchain, in: Proceedings of the 43rd IEEE/ACM International Conference on Software Engineering:
59. Wang, D., Wu, S., Lin, Z., Wu, L., Yuan, X., Zhou, Y., Wang, H., Ren, K., 2021. Towards a first step to understand flash loan and its applications, in defi ecosystem, in: Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing (SBC), pp. 23–28.
60. Wang, S.H., Wu, C.C., Liang, Y.C., Hsieh, L.H., Hsiao, H.C., 2021. Promutator: Detecting vulnerable price oracles in defi by mutated transactions, in: Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 380–385.
61. Werner, S.M., Perez, D., Gudgeon, L., Klages Mundt, A., Harz, D.,et al, K., 2021. Sok: Decentralized finance (defi). arXiv preprint arXiv:2101.08778 doi:https://doi.org/10.48550/arXiv.2101.08778.
62. Winter, P., Lorimer, A.H., Snyder, P., Livshits, B., 2021. What's in your wallet? privacy and security issues in web 3.0. arXiv preprint arXiv:2109.06836 doi:https://doi.org/10.48550/arXiv.2109.06836.
63. WorldBank Blogs, 2012. Latin America: Most still keep their money under the mattress. URL: https://blogs.worldbank.org/latinamerica/latin-america-most-still-keep-their-money-under-the-mattress [Accessed 8 August, 2022]
64. Xue, Y., Ma, M., Lin, Y., Sui, Y., Ye, J., Peng, T., 2020. Cross-contract static analysis for detecting practical reentrancy vulnerabilities in smart contracts, in: Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 1029– 1040.
65. Yazdanparast, E., 2021. All you need to know about defi flash loans.URL: https://medium.com/coinmonks/all-you-need-to-know-about-defi-flash-loans-ca0ff4592d90. [accessed on 21 May, 2022].