CIS-TC Newsletter

Communications and Information Security Technical Committee

http://cis.committees.comsoc.org/

Issue 8 – July 2021

cistc@comsoc.org

http://cis.committees.comsoc.org/newsletters

Contents

Message from the Chair

Dear CISTC Members,

I would like to sincerely welcome you to the present issue of CIS-TC Newsletter. In 2016, we started to plan it as a mean to share relevant information among the Members of our Committee twice per year to coincide with the meeting at ICC and Globecom conferences. However, the global pandemic compelled the remote rescheduling of all the IEEE 2020 events, and, consequently, our meetings has become *virtual* events; as a consequence, our Newsletter could be considered an essential way to reshape relationships within our communities via a wider and more structured social internetworking.

In this perspective, we are expected to improve to improve the level of interactive discussion by using this Newsletter as an *open* and *inclusive* platform *in progress* where all the Members of our Community are welcome to cooperative contribute to imagine *our* future. Please feel free to send us any scientifical, technical contributions or even news that you believe could be beneficial to our community.

Let me conclude this message wishing you to enjoy in reading this Issue, while having good summer holidays, together with your family and friends,

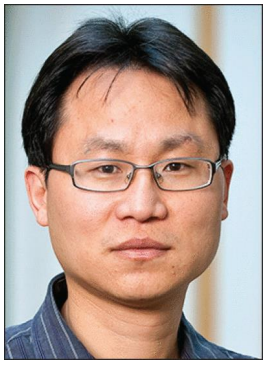
Sincerely,
Francesco Chiti
Chair of CIS-TC

CISTC Technical Recognition Award 2021

The Award Committee chaired by Professor Abderrahim Benslimane, with unanimous consent decided to give CIS-TC Technical Recognition Award 2021 to Professor Xiaodong Lin at the University of Guelph (Canada) for "his contribution to security field".

The Award recognizes members of the IEEE Communications Society, who have made outstanding contributions to the scientific and technological advancement of security.

The Committee congratulate with the Awarded and, due to the global pandemic, he will be hopefully awarded during the CIS-TC meeting held at IEEE Globecom 2021 in Madrid, Spain.



Xiaodong Lin *received his Ph.D. degree (with the Outstanding Achievement in Graduate Studies Award) in Electrical and Computer Engineering from the University of Waterloo, Canada, in 2008. He is currently a full Professor in the School of Computer Science, University of Guelph, Canada. His research interests include wireless communications and network security, computer forensics, privacy-enhancing technologies, Blockchain and applied cryptography. He is a Fellow of the IEEE.*

FEATURED TOPICS

"Decentralized Finance and Security"

Rundong Gan[1] and Xiaodong Lin[1]
[1]School of Computer Science at the University of Guelph, Guelph, Canada

Abstract—Decentralized Finance (DeFi), a new form of finance, took shape in 2020 and is continuously expanding. The total amount of value locked (TVL) inside DeFi protocols has reached an astounding number of $85.63 billion as of August 2021, showing the exponential growth of the DeFi industry. However, its growth has attracted the attention of malicious actors and DeFi security incidents are frequent. In this article, we introduce the basic knowledge of DeFi, enumerate some known attacks, and suggest future directions to improve the security of decentralized finance.

Index Terms—DeFi Security, DeFi Attacks, Blockchain Security, Cryptocurrency Application

I. INTRODUCTION

Decentralized Finance (DeFi) is a new developing area at the intersection of peer-to-peer networks, cryptography, digital assets, and financial services. Different from Centralized Finance (CeFi), DeFi keeps the business reputation with smart contracts and DeFi protocols instead of central institutions or a middleman. The revolutionary design has attracted more and more investors and developers, and many DeFi applications have also been deployed on blockchains [1].

Due to the novelty of DeFi, some risks are still unknown. Most of DeFi projects are launched with a focus on availability and profitability and less on security. At the same time, the open-source code of DeFi projects enables attackers to locate vulnerabilities quickly and efficiently. Unlike traditional system attacks, hackers can directly obtain a large number of economic benefits from DeFi attacks. Until now, DeFi systems have suffered from numerous attacks [2], and the biggest loss reached $600 million [3]. Therefore, there is a critical need for security research of DeFi.

To help readers understand DeFi security, we briefly introduce DeFi, enumerate some representative attacks, and suggest some research directions of DeFi security.

II. DECENTRALIZED FINANCE

A. What is DeFi

Decentralized Finance (DeFi) is a general term for decentralized financial applications [4] and these applications are composed of smart contracts and DeFi protocols. DeFi provides various financial services including payments, trading, lending/borrowing, derivatives, options, insurance, asset management, etc. Different from centralized finance, DeFi applications operate on blockchains (primarily Ethereum) with- out centralized intermediaries such as brokerages, centralized exchanges, or banks and enable the provisioning of financial services anywhere for anyone regardless of ethnicity, age, or cultural identity.

B. DeFi Applications

Like traditional finance, DeFi applications can also be categorized by the type of services they provide [5]. Representative categories are shown below:

- **Exchanges**. Decentralized exchanges (DEXs) are a class of DeFi applications that facilitate the buying and selling of digital assets on blockchains. DEXs are non-custodial and do not have ownership over a user's funds at any point in time. All DEX trades are settled on blockchains, thereby ensuring public verifiability for all transactions to network nodes. As there are no centralized intermediaries, DEXs require special mechanisms for price discovery, and these mechanisms can be divided into two categories: Order Book and Automated Market Makers (AMMs). Among them, Automated Market Makers (AMM) based DEXs are on the ascendancy, with an aggregate value locked exceeding 15 billion USD [6].
- **Lending & Borrowing**. Lending & Borrowing facilitate risk-taking and expand the supply of capital through leverage, playing an important role in financial markets. The classic form of centralized lending & borrowing is banking, and banks manage all assets, interest rates and borrowers' credit-worthiness. By contrast, decentralized lending & borrowing applications use smart contracts to implement all business logic. Over collateralized loans and flash loans are two general loan forms of DeFi lending & borrowing [5].
- **Derivatives**. Like traditional finance products, decentralized derivatives are also synthetic financial instruments whose value is based on a function of an underlying asset or group of assets. Common examples of DeFi derivatives are futures,

options, and synthetic assets [7], which reference the value of an asset at some time in the future.

- **Oracle**. An Oracle [8] is a mechanism that imports off-chain data (such as off-chain asset prices) into the blockchain so that it is readable by smart contracts. Oracles are relied upon by various DeFi applications (e.g. exchanges, lending & borrowing, derivatives).

C. Differences between DeFi and CeFi

Although DeFi and CeFi have many financial applications with same financial concepts, they are still fundamentally different [4] [9]. The most important differences between them are listed in Table I.

TABLE I
THE DIFFERENCES BETWEEN DEFI AND CEFI

	Decentralized Finance (DeFi)	Centralized Finance (CeFi)
Custody of Assets	Assets are held directly by users in non-custodial wallets or via smart contract-based escrow.	Assets are held by a regulated service provider or custodian on asset owners' behalf.
Transparent and Accountable	All transactions are transparent and can be observed and tracked by anyone.	Only the service provider can observe and track transaction information.
Governance and Regulation	Managed by protocol developers or determined by users holding tokens granting voting rights, and lack of legal regulation.	Specified by the rules of the service provider, market-place, regulator and/or self-regulatory organization, and the relevant legislation is well established.
Auditability	Open-source codes and public ledgers allow anyone to verify protocols and activities.	In general, only authorized third-party auditors can audit the source code and related data.
Risk Factor	Security relies on the technology users are using.	Service providers are responsible for security.

III. DeFi SECURITY

Permissionless blockchains such as Ethereum perform well in decentralized finance. However, it is no secret that the DeFi system on permissionless blockchains is a highly adversarial environment: when a DeFi application can be used for financial services, it also can be exploited for illegal profit [10] [11]. Some people have characterized the peer-to-peer finance system as a dark forest [12] [13], where vulnerable DeFi applications and innocent users represent prey and malicious actors play the role of predators, respectively. An advanced predator will track down any valuable transactions and DeFi applications and uses software technology and financial tools to plunder assets. At the same time, due to the lack of legal regulation, exploiting DeFi projects is currently a low-risk high reward opportunity to malicious actors.

In this section, we list representative attack techniques used in DeFi security incidents and disclosed by security researchers.

A. Smart Contract Attacks

Smart contracts are the basis of DeFi applications and any code-level vulnerabilities of them can be exploited. In many situations, hackers can gain unauthorized access to DeFi applications by attacking the weak code, and then they can transfer all virtual assets from these applications to their own blockchain addresses. The code vulnerabilities of smart contracts have been extensively discussed in previous work [14] [15]. In the early development of DeFi, some simple attacks caused devastating damage to DeFi applications, such as reentrancy attack [16] and integer overflows attack [17].

When adhering to safe coding practices, the risk of these attacks can be mitigated. However, because of the quick and hasty development driven by a fear of missing out profit opportunities, some logical bugs are still hard to avoid and can be exploited by hackers. In September 2020, the bZx, a famous lending application, suffered a loss of over 8 million USD just due to a trivial logic error [18], despite having been audited twice by third-party code auditors.

B. DeFi Protocol Attacks

Protocols are core logic of DeFi applications. DeFi projects are launched on blockchains without intermediary intervention and can't be revised, so all possible scenarios should be considered in DiFi protocols before these projects are deployed. However, to reduce the cost of gas fees, most DeFi projects only have a few thousand lines of code or less. This always makes DeFi contracts flawed and many extreme cases are ignored. Crafty hackers can find flaws in open-source codes and construct extreme transactions to attack DeFi protocols. In June 2020, hackers initiated a special transaction of the STA token to the decentralized exchange Balancer. STA is a deflationary cryptocurrency, which will be partially destroyed in each transaction. Due to the lack of special handling of deflationary cryptocurrencies, Balancer eventually lost $500,000 worth of virtual assets [19].

Unlike smart contract attacks, DeFi protocol attacks focus on vulnerabilities of protocol design. For different DeFi protocols, the forms of attacks are completely disparate [20].

C. Market Manipulation Attacks

Market manipulation refers to artificial inflation or deflation of the price of a financial product. In traditional finance, manipulators enter crafted buy/sell orders to control the stock price. In DeFi, the cryptocurrency price can be manipulated in the same way. Differently, DeFi market manipulation is more complex and diverse. As a result, the manipulators can be traders, market makers, exchange managers, or even the government. Due to the financial attributes of DeFi, manipulation is a very common practice in decentralized financial systems. There are three common methods of market manipulation.

- **Pump and Dump Scheme-based Manipulation**. In a pump and dump scheme, fraudsters typically spread false or misleading information on social networks to create a buying frenzy that will "pump" up the price of a stock and then "dump" the price by selling their own products at the inflated price. The manipulation is often seen in stock markets [21] and centralized cryptocurrency exchanges [22], but it can equally be used in decentralized financial systems.
- **Wash Trading-Based Manipulation**. To perform wash trading, several users collude and trade only amongst themselves.

Thereby, they give the impression that they are buying and selling, but in reality, they are not changing their own positions or taking any real market risk. These activities inevitably lead to increased trading volume, a metric that is observed by other traders and may influence the price of virtual assets. This manipulation is common in Order Book-based DEXs [23].

- **Flash Loan-based Manipulation**. Firstly, attacker takes out a flash loan (a form of uncollateralized lending) from a DeFi application. Secondly, a portion of the borrowed capital is used to manipulate an Oracle's price, and another portion is used to arbitrage from the Oracle-based DeFi applications. Finally, the attacker pays the borrowed capital back in the same transaction, and the balance is the profit of this attack. This manipulation is usually focused on AMM-based DEXs [11].

D. Transaction Ordering Attacks

On blockchains, transactions are executed sequentially according to how they have been ordered in a block. Front-running a transaction refers to submitting a transaction which is solely intended to be executed before some other pending transactions, and back-running a transaction is the opposite. If an attacker wants to benefit from front-running transactions, he or she would have their transactions executed before a victim transaction. Similarly, the attacker can also benefit from back-running transactions. As transactions are ordered by their gas price [24], the attacker can manipulate the order of attack transactions relative to the target transactions by setting a higher or lower gas price. The attacks which involve front- and/or back-running within a single block and destroy the security of DeFi are called transaction ordering attacks. Classic transaction ordering attacks include front-running attacks [25] and sandwich attacks [10].

IV. FUTURE RESEARCH DIRECTIONS

In this section, we propose some possible future directions to improve the security of DeFi.

A. Program Analysis with Advanced Semantics

There is a large amount of work both in academia [14][26] and industry [27] to analyze smart contract bugs and vulnerabilities. However, while smart contract analysis tools keep improving, the number and scale of smart contract exploits have not significantly decreased [28]. This is because few tools analyze smart contracts from advanced semantic properties, such as how an extreme transaction execution path influence the balances and prices of cryptocurrencies. Further, it is impossible for existing smart contract analysis tools to understand the composable nature of smart contracts and infer complex scenarios where the issue happens due to some changes external to the smart contracts.

B. Reliable DeFi Protocols

The ongoing DeFi development involves composition of DeFi apps and financial primitives as 'Money Legos' [4]. Each individual DeFi app, called "Lego brick", is a specific financial product or service that can be freely combined with others. While the 'Money Legos' architecture is advantageous in many respects, a deficiency in one protocol might cause failure of the whole protocol stack. For example, in August 2021, hackers exploited a vulnerability in Poly Network (a DeFi protocol that provides cross-chain trading services) and obtained $600 million worth of cryptocurrencies [3] from different heteroid blockchains which all have deployed smart contracts of Poly Network.

Therefore, the reliability of DeFi protocols is very important. In particular, some basic protocols of DeFi should be improved as soon as possible:

- **Oracle Protocols**. Many DeFi apps rely on Oracles' prices but attacking Oracles for profit is frequent in current blockchain system [29]. Now an open challenge is how to design new Oracle protocols to escape manipulations.
- **Cross-chain Protocols**. Cross-chain Protocols aim to achieve secure trading between different types of cryptocurrencies. In academia, there are only a few studies on cross-chain transactions [30].
- **AMM Protocols**. With a focus on availability and profitability and less on security, many AMMs are frequently attacked and manipulated [6].

C. Composability Risk Assessment

In DeFi 'Money Legos', a new DeFi app may combine many specific-purpose Lego-brick products and services into a more complex product that is even more powerful or customized to specific user needs. This enables a level of flexibility and innovation that is unthinkable with traditional financial systems that are protected by the firewalls of banks [31].

However, 'Money Legos' can expose agents to compos- ability risk, which is unquantified in most DeFi projects. An example of composability risk is the use of flash loans for manipulating AMMs and financially exploiting protocols that use those AMMs as price feeds [32]. Although composability- based manipulation attacks have already appeared, there is still a significant gap in DeFi research to assess and quantify composability risk of projects.

D. Anonymity and Privacy

At present, the anonymity and privacy of DeFi is a significantly unexplored field. Although privacy protection may help malicious users to escape the consequences of their actions, it is still valuable and expected in real DeFi trading. More users hope to hide their identities and transaction content to avoid unnecessary trouble. However, due to the large computational cost of smart contracts, some privacy protection techniques (e.g., zero-knowledge, multi-party computations) cannot be directly used on DeFi system. Therefore, lightweight DeFi protocols for privacy protection need to be devised in the future.

V. CONCLUSION

The DeFi system based on blockchains is a complex and adversarial environment. In this system, protocols might fail, markets can be manipulated, and assets in virtual wallets are at risk of being stolen. Maintaining DeFi security is a challenging but interesting problem. In this article, we have enumerated attacks to DeFi projects, as well as future research directions to solve these security questions. We hope

that our introduction can bring new inspiration to the research of DeFi and security.

REFERENCES

[1] DeFi-Plus, "The list of DeFi Projects." https://defipulse.com/, 2021.
[2] Slowmist, "Defi hack events." https://hacked.slowmist.io/en/, 2021.
[3] CoinDesk, "Cross-chain defi site poly network hacked; hundreds of millions potentially lost: Hundreds of millions potentially lost." https://www.coindesk.com/cross-chain-defi-site-poly-network-hacked.
[4] W. S. of the University of Pennsylvania, "DeFi Beyond the Hype: The Emerging World of Decentralized Finance." https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf, 2021.
[5] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "Sok: Decentralized finance (defi)," arXiv preprint arXiv:2101.08778, 2021.
[6] J. Xu, N. Vavryk, K. Paruch, and S. Cousaert, "Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols," arXiv preprint arXiv:2103.12732, 2021.
[7] Synthetix, "Synthetix-decentralised synthetic assets." https://www.synthetix.io, 2020.
[8] A. Beniiche, "A study of blockchain oracles," arXiv preprint arXiv:2004.07140, 2020.
[9] K. Qin, L. Zhou, Y. Afonin, L. Lazzaretti, and A. Gervais, "Cefi vs. defi–comparing centralized to decentralized finance," arXiv preprint arXiv:2106.08157, 2021.
[10] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, "High-frequency trading on decentralized on-chain exchanges," arXiv preprint arXiv:2009.14021, 2020.
[11] K. Qin, L. Zhou, B. Livshits, and A. Gervais, "Attacking the defi ecosystem with flash loans for fun and profit," arXiv preprint arXiv:2003.03810, 2020.
[12] R. Dan and K. Georgios, "Ethereum is a dark forest." https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest/, 2021.
[13] K. Qin, L. Zhou, and A. Gervais, "Quantifying blockchain extractable value: How dark is the forest?," arXiv preprint arXiv:2101.05511, 2021.
[14] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and M. Vechev, "Securify: Practical security analysis of smart contracts," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 67–82, 2018.
[15] Z. A. Khan and A. S. Namin, "A survey on vulnerabilities of ethereum smart contracts," arXiv preprint arXiv:2012.14481, 2020.
[16] N. F. Samreen and M. H. Alalfi, "Reentrancy vulnerability identification in ethereum smart contracts," in 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pp. 22–29, IEEE, 2020.
[17] E. Lai and W. Luo, "Static analysis of integer overflow of smart contracts in ethereum," in Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, pp. 110–115, 2020.
[18] PeckShield, "bzx hack full disclosure (with detailed profit analysis)." https://peckshield.medium.com/bzx-hack-full-disclosure-with-detailed-profit-analysis-e6b1fa9b18fc, 2020.
[19] CoinDesk, "Hacker drains 500k dollars from defi liquidity provider balancer." https://www.coindesk.com/hacker-drains-defi-liquidity-balancer, 2020.
[20] K. Oosthoek, "Flash crash for cash: Cyber threats in decentralized finance," arXiv preprint arXiv:2106.10740, 2021.
[21] Y. C. Huang and Y. J. Cheng, "Stock manipulation and its effects: pump and dump versus stabilization," Review of Quantitative Finance and Accounting, vol. 44, no. 4, pp. 791–815, 2015.
[22] J. Xu and B. Livshits, "The anatomy of a cryptocurrency pump-and-dump scheme," in 28th USENIX Security Symposium (USENIX Security 19), pp. 1609–1625, 2019.
[23] F. Victor and A. M. Weintraud, "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in Proceedings of the Web Conference 2021, pp. 23–32, 2021.
[24] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," arXiv preprint arXiv:1904.05234, 2019.
[25] S. Eskandari, M. Moosavi, and J. Clark, "Sok: Transparent dishonesty: front-running attacks on blockchain," 2019.
[26] A. Permenev, D. Dimitrov, P. Tsankov, D. Drachsler-Cohen, and M. Vechev, "Verx: Safety verification of smart contracts," in 2020 IEEE Symposium on Security and Privacy (SP), pp. 1661–1677, IEEE, 2020.
[27] Consensys, "Mythx: Smart contract security service for ethereum." https://mythx.io/, 2021.
[28] C. Ferreira Torres, A. K. Iannillo, A. Gervais, et al., "The eye of horus: Spotting and analyzing attacks on ethereum smart contracts," in International Conference on Financial Cryptography and Data Security, Grenada 1-5 March 2021, 2021.
[29] S. Eskandari, M. Salehi, W. C. Gu, and J. Clark, "Sok: Oracles from the ground truth to market manipulation," arXiv preprint arXiv:2106.00667, 2021.
[30] H. Tian, K. Xue, X. Luo, S. Li, J. Xu, J. Liu, J. Zhao, and D. S. Wei, "Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol," IEEE Transactions on Information Forensics and Security, 2021.
[31] Radix, "What is defi composability and why does it matter?." https://www.radixdlt.com/post/ what-is-defi-composability-and-why-does-it-matter, 2020.
[32] Y. Cao, C. Zou, and X. Cheng, "Flashot: A snapshot of flash loan attack on defi ecosystem," arXiv preprint arXiv:2102.00626, 2021.

FORTHCOMING MEETING

The next IEEE ComSoc's Communication & Information Security TC (CISTC) meeting will be held at IEEE GC 2021 "Connecting Cultures around the Globe,", 7-11 December 2021 (Madrid, Spain). You are more than welcome to join it and to provide your valuable contribution.

IEEE GLOBECOM
IEEE Global Communications Conference
7-11 December 2021 // Madrid, Spain
Connecting Cultures around the Globe

FEATURED TOPICS

"Cyber Security and Critical infrastructure Protection: Opportunities and Future Prospective"

Brij Gupta[1]
[1]National Institute of Technology Kurukshetra, Haryana, India

Abstract:

Today, computers are increasingly being used for storing and retrieving information. Some of this information is of a sensitive nature requiring adequate security measures to safeguard the sensitive information. It has also brought unparalleled and potential challenges with them. Moreover, attackers keep changing their attack strategies rapidly to hide their actual identity. In addition, cyber space is considered the fifth battle-field after land, air, water and space. Therefore, strengthening the security has become a vital homeland security mission and critical infrastructure protection. Security Challenges is the protection of information systems, hardware, software, and information as well from theft, damages, interruption or misdirection to any of these resources and critical infrastructures. Therefore, to protect against various attacks, security specialists need to keep concocting new schemes to control any new attacks. While protecting against naïve attacks, some type of advanced techniques should be included in the lineup of security tools or software. Hence, in this talk, I will introduce the principles of cyber security aspects and awareness about the various tools and techniques for securing the information from a variety of attacks against critical infrastructure. Moreover, I will also discuss various security solutions to protect various critical infrastructures against these attacks.

CIS-TC ORGANIZED SYMPOSIA

- *Communications and Information System Security Symposium* – **Globecom2021,** 7-11 December 2021, Virtual Conference - 7-11 December 2021 - Madrid, Spain, Hybrid: In-Person and Virtual Conference "*Connecting Cultures around the Globe*,", (https://globecom2021.ieee-globecom.org)
- *Communications and Information System Security Symposium* – **ICC2022**, 16-20 May 2022 - Seoul, South Korea, Hybrid: In-Person and Virtual Conference "*Intelligent Connectivity for Smart World*" https://icc2022.ieee-icc.org)

CIS-TC AFFILIATE CONFERENCES

- **Conference: ICACT2021**
  - 23rd International Conference on Advanced Communications Technology (ICACT2021)
  - Febuary 7- 10, 2021, Online Virtual Conference
  - http://www.icact.org
- **Conference: WiMob 2021**
  - 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2021)
  - October 11 – 13, 2021, Bologna, Italy
  - http://www.wimob.org/wimob2021
- **Conference: CSNET 2021**
  - 5th Cyber Security in Networking Conference (CSNET 2021)
  - October 12 – 24, 2021, Abu Dhabi, UAE (Hybrid Conference)
  - https://csnet-conference.org/2021