Unraveling the Structure of Nested Decentralized Finance (DeFi) Protocols

By Stefan Kitzler (Complexity Science Hub Vienna and AIT - Austrian Institute of Technology), Friedhelm Victor (Technische Universität Berlin), Pietro Saggese (Complexity Science Hub Vienna and AIT - Austrian Institute of Technology), and Bernhard Haslhofer (Complexity Science Hub Vienna)

Decentralized Finance (DeFi) protocols offer financial services such as lending or trading, without intermediaries, on distributed ledgers like Ethereum. They are implemented as software programs by one or more smart contracts. A DeFi composition is a novel form of software-driven financial engineering where financial service providers can combine the financial functions of several DeFi protocols to offer novel, complex, and deeply nested financial products without being dependent on any single intermediary. We conducted a measurement study on such compositions, using a dataset of 23 labeled DeFi protocols and 10,663,881 associated Ethereum accounts. DeFi compositions can be compared to constructions of building blocks, i.e., "financial bricks" that can be arbitrarily assembled: we propose an algorithm to decompose a transaction to a DeFi protocol into nested building blocks that may be part of other DeFi protocols. Understanding DeFi compositions is of great importance, as they may impact the system interoperability, are increasingly integrated with web technologies, and may introduce risks through complexity and leverage.

1. Introduction

Decentralized Finance (DeFi) is a new financial paradigm for conducting financial activity without intermediaries. Building upon innovative distributed ledger technologies (DLTs), it aims to disrupt the traditional financial market. At the time of writing, Ethereum[1] is the most relevant DLT for DeFi. The Ethereum DeFi ecosystem comprises multiple DeFi protocols, that is, DeFi applications that provide one or more decentralized financial services to their customers: DeFi protocol users can lend and exchange cryptoassets, or issue derivatives contracts on underlying cryptoassets to bet on their future price changes. The financial services are implemented as one or more smart contracts, that is, computer software programs that run on the Ethereum DLT and encode the logic of conventional financial operations. Smart contracts are automated, facilitate re-usability, and their output is deterministic. Decentralization ensures that financial transactions are settled without resorting to a central authority. Automation implies that DeFi users do not interact with other customers, but rather with the protocol itself.

DeFi users can also combine different DeFi services to create new financial products, also known as DeFi compositions, within one single transaction. For example, aggregator services like the *1inch* DeFi protocol search for optimal prices across multiple decentralized exchange platforms (DEXs) and automatically route users to the one offering the best price at the transaction time. Most importantly, routing and settling can occur within the same Ethereum transaction.

Our study looks at such interactions between DeFi protocols from multiple aspects[2]. First, from a higher perspective, we reconstruct the network of interacting smart contracts and their associated protocols. Second, we look at individual transactions to identify and quantify the DeFi protocol compositions within Ethereum transactions. This allows us to identify the DeFi building blocks, that is, sets of smart contracts that are used together to provide core financial functionalities such as the exchange of two cryptoassets, or their lending. These building blocks can be nested inside other building blocks that provide more complex financial services. Finally, we present a case study inspired by the recent collapse of the TerraUSD (UST) stablecoin[3] to investigate if and what DeFi protocols are especially intertwined with stablecoins.

The main contributions of our work are the following:
- We provide a manually curated ground truth of 1407 smart contracts associated to 23 DeFi protocols and derived 10,663,881 associated Ethereum smart contracts.
- We analyze the smart contract network and find that existing algorithms indicate the existence of DeFi compositions.
- We develop a novel algorithmic method to identify and understand protocol compositions. We find that the most frequent financial activity conducted is the exchange of cryptoassets.
- We present a case study illustrating how a hypothetical run on the stablecoin Tether would affect the building blocks of individual DeFi protocols.

---

[1] See Buterin, Vitalik. "A next-generation smart contract and decentralized application platform". *white paper* 3.37 (2014): 2-1.

[2] See Kitzler, S., Victor, F., Saggese, P., & Haslhofer, B. (2022). "Disentangling decentralized finance (defi) compositions". *ACM Transactions on the Web* (*TWEB).*

[3] See Briola, A., Vidal-Tomás, D., Wang, Y., & Aste, T. (2023). "*Anatomy of a Stablecoin's failure: The Terra-Luna case*". *Finance Research Letters*, 51, 103358.

2. Motivation

The investigation of DeFi compositions is relevant in many aspects. First, whilst DeFi protocols offer new opportunities, their composability entails enormous additional complexity and opaqueness to an already complex cryptoasset ecosystem, which currently has a market valuation of about 1T USD[4]. Similarly to the financial crisis that hit the global financial system in 2007[5], these instruments are highly profitable yet little understood by expert traders, let alone by non-professional investors. If these protocols are not understood and adopted more broadly, they could have unforeseeable systemic effects on financial markets and our society.

Furthermore, cryptoassets have started integrating with other non-DLT-based technology, and especially with traditional finance: stablecoins are cryptoassets that maintain the peg to an asset like the US dollar, and centralized exchanges like Binance or the recently collapsed FTX provide cryptocurrency investors with interfaces to conventional payment systems[6]. Systemic risk might stem from links between these actors, and DeFi composability might act as an echo chamber.

Finally, composability may impact the development of ecosystem interoperability. For instance, identifying frequently used compositions may help identify novel relevant compositions.

3. Data

To study DeFi compositions, we collected blockchain transactions between Ethereum smart contracts associated with known DeFi protocols. We started by constructing a ground truth dataset of smart contracts that were manually inspected and associated with given DeFi protocols. We focused on the most relevant protocols for market capitalization between March 2021 and August 2021. We defined a set of 23 DeFi protocols and identified 1407 associated smart contracts. We extended this list by implementing a heuristic based on smart contract creations. Then we extracted all transactions on the Ethereum blockchain from 01-Jan-2021 (block 11,565,019) to 05-Aug-2021 (block 12,964,999) and filtered only the transactions involving the addresses of interest. For each transaction, we extracted multiple variables such as the source and destination addresses, the transaction hash, or the trace ID.

4. Network Analysis

To investigate the smart contract interactions from a higher-level perspective, we constructed a network abstraction in which nodes are smart contracts, and the edges are links between smart contracts that interact with each other within one single transaction. This network represents interactions between protocols at the smart contract level.

---

[4] Coinmarketcap. Market capitalization. See https://coinmarketcap.com/charts/.

[5] See Martin Neil Baily, Robert E. Litan, and Matthew S. Johnson. 2008. "The Origins of the Financial Crisis". *Technical Report. Brookings Institution*.

[6] See Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2023). "The Technology of Decentralized Finance (DeFi)". *BIS Working Papers*.

We focused on targeted metrics that provide relevant insights on composability aspects[7]. Analyzing the degree distribution and centrality measures can help identify the smart contracts implementing core functionalities. We found that the degree follows a power-law distribution, and that the most connected nodes are smart contracts associated with decentralized exchanges and lending protocols such as *UniSwap* and *Aave*. Similar results were obtained by investigating what are the most central nodes according to different centrality measures, letting hypothesize that these smart contracts are part of DeFi compositions.

Next, we looked at metrics to analyze how smart contracts fall into different network components, that is, parts of the network in which all nodes can reach the nodes of that sub-network through link connections. Interestingly, in the second-largest component we found addresses of all the analyzed protocols except for one (*RenVM*). This component encompasses most protocol interactions.

Finally, we exploited algorithms to categorize nodes in communities based on structural similarities to investigate whether the communities correspond to DeFi protocols. The findings show that such algorithms cannot disentangle DeFi protocols, but rather indicate protocol composition patterns.

5. Building Block Extraction

After analyzing the macroscopic network perspective, we investigated the microscopic level by looking at individual Ethereum transactions, aiming to identify the DeFi building blocks. Building blocks are a basic set of smart contracts that, in combination, provide core financial functions of the DeFi ecosystem, such as trading two cryptoassets.

We recall that, within one single Ethereum transaction, one smart contract can interact with many other smart contracts belonging to multiple DeFi protocols. We thus developed an algorithm that inspects each transaction and identifies a composition every time a smart contract of one protocol interacts with another protocol-specific smart contract.

With more than 21 million occurrences, the most frequent building block is associated with the decentralized exchange *UniSwap* and enables the trade of cryptoassets. Another relevant building block in terms of occurrences is associated with the *0x* protocol and provides a financial function that allows withdrawing funds.

The most relevant pattern we discovered by investigating the building blocks is that they can be nested within each other. In other terms, when a user interacts with the smart contract of one DeFi protocol, the interaction could trigger subsequent cascading actions involving smart contracts belonging to other DeFi protocols. We show this concept in Figure 1. To construct it, we collected all the transactions directed to one lending service protocol, *Aave*. The plot shows a user (EOA) interacting with *Aave*, represented by the first light-blue node on top. All subsequent nodes represent other DeFi protocols that can be combined with *Aave* within one single transaction. For instance, in the far-right branch we see that it is possible to create compositions of the lending service Aave with the decentralized exchange *SushiSwap* (dark purple), and then with *Synthetix* (light purple), a protocol that offers derivatives contracts on cryptoassets.

Figure 1: The space of possible compositions with Aave
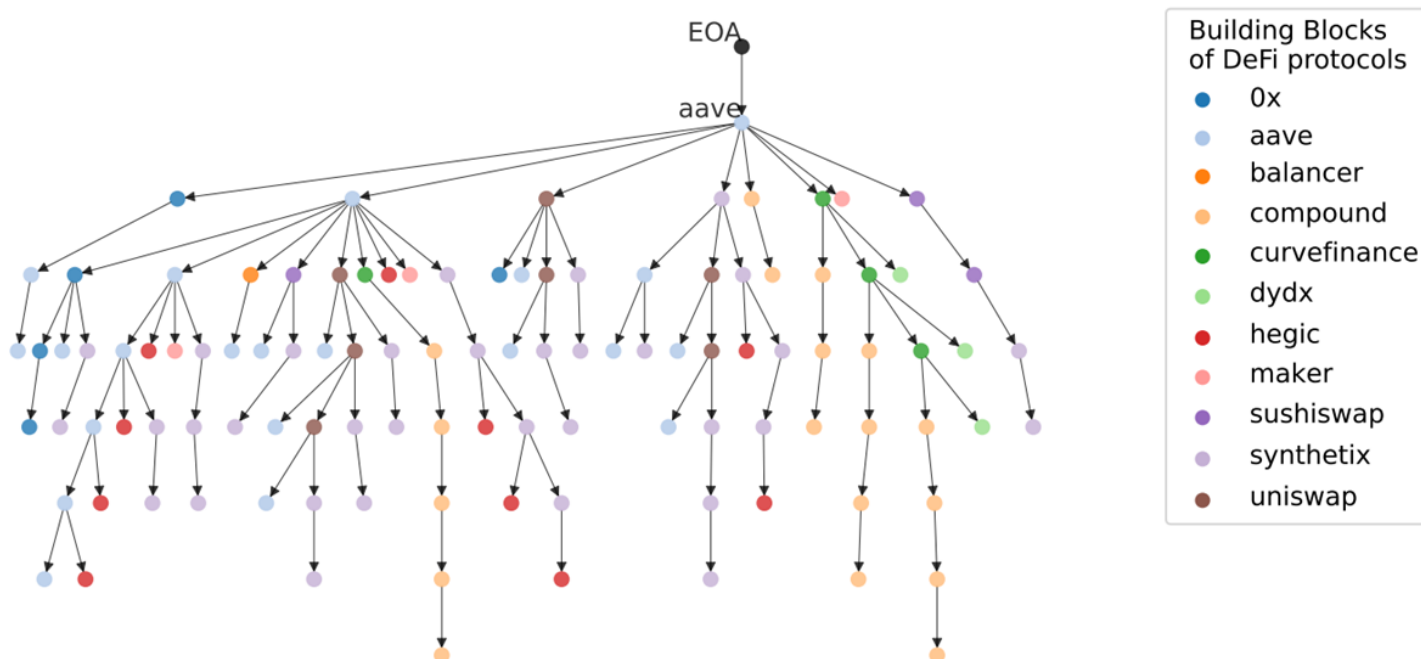
Notes: Each node represents a building block, each link a possible nested building block, extracted from all transactions to Aave. We observe for this protocol a maximum depth of seven nested DeFi building block levels.

6. Stablecoins and Bank Run Risk

Stablecoins are cryptoassets whose value is anchored to another asset, and their value should be stable by design[8]. However, events like the collapse in May 2022 of the Terra ecosystem and its stablecoin TerraUSD (UST), which maintained its peg to the US dollar, show that stablecoins are less stable than they are supposed to be. An initial de-peg of the UST stablecoin from the US dollar led many investors to close their positions in UST. This eventually led to a stablecoin run, akin to a bank run, and the price of the stablecoin went to zero within few hours.

Motivated by this recent demonstration of systemtic risk associated with stablecoins, we measured how a hypothetical run on the stablecoin Tether (USDT) would affect the DeFi protocols investigated in our analysis. We analyzed, for each protocol, the fraction of building blocks containing the USDT asset directly or indirectly (that is, in more deeply nested building blocks). Figure 2 shows the results. While most protocols have relatively low dependencies (< 10%), the decentralized exchanges *SushiSwap* and *Curvefinance* strongly depend on USDT.

---

[8] See Moin, A., Sekniqi, K., & Sirer, E. G. (2020). "SoK: A classification framework for stablecoin designs". *In Financial Cryptography and Data Security: 24th International Conference, FC 2020*, Kota Kinabalu, Malaysia.

**Figure 2: Fraction of building blocks associated to 23 DeFi protocols
in our sample that depend on the USDT cryptoasset**
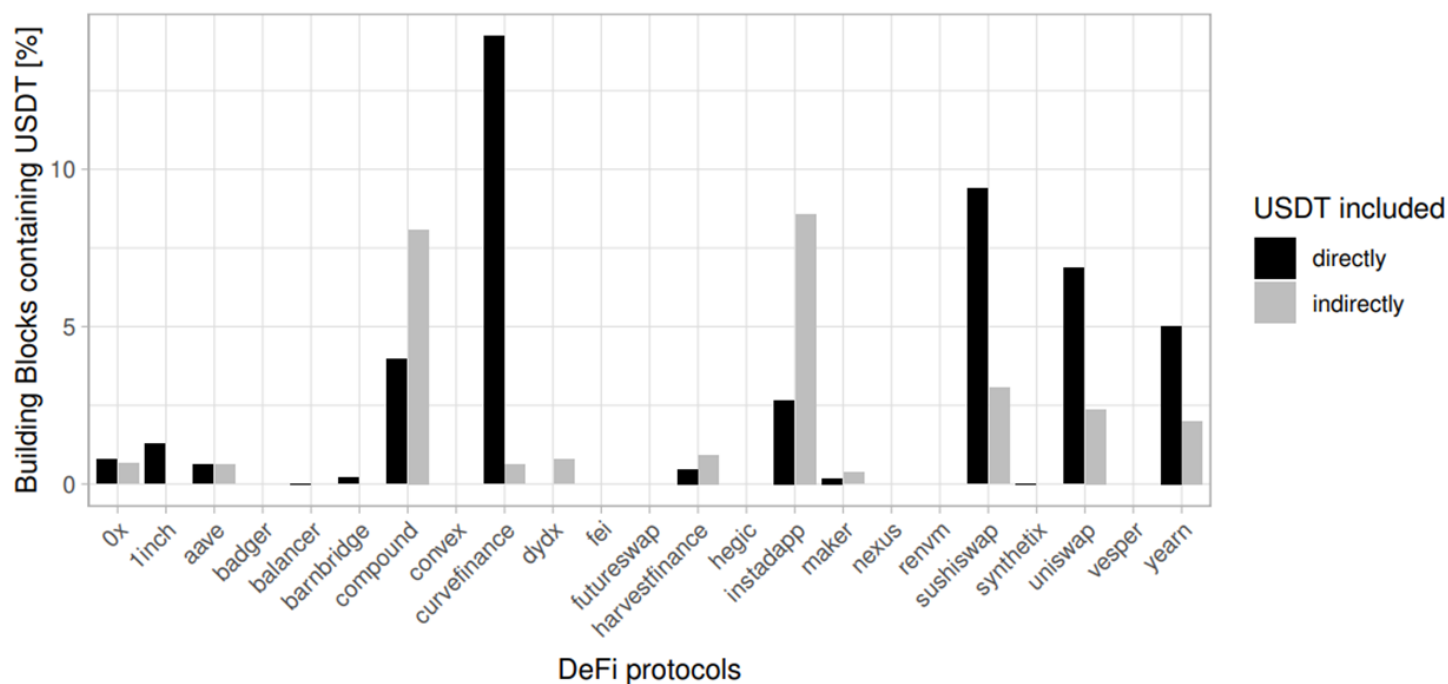
Notes: *We distinguish between those that include the cryptoasset directly (black), or indirectly (gray) through other nested blocks.*

7. Discussions and Future work

The consequences of the collapse of Terra and the failure of the cryptocurrency exchange FTX demonstrate that the crypto ecosystem is highly entangled and susceptible to contagion dynamics. Decentralized Finance adds an additional layer of complexity – and risk. Our work shows that DeFi protocols are highly interconnected: users can construct financial products that are complex and whose risks are not yet fully understood. DeFi services can be imagined as a construct of nested building blocks, heavily dependent on very specific basic "financial bricks". Yet, whilst individual DeFi protocols have been studied in detail, little is known about how they interoperate. The consequences on the stability of the DeFi ecosystem, should one or multiple of these basic financial bricks "fail", must still be investigated in depth.

As the financial crisis in 2008 has shown, a lack of understanding and regulation can have unforeseeable risks for the financial markets. DeFi protocols are interwoven in highly complex transactions and poorly understood financial products: our work contributes to identifying the core DeFi building blocks and lays the groundwork for a better understanding of systemic risk in DeFi. ■

About the authors

Stefan Kitzler received a bachelor's and a master's degree in Technical Physics from TU Vienna. During his studies, he did an internship at the AIT Austrian Institute of Technology and continued the cooperation with the AIT for his master's thesis "Reliability in power electronics for electric energy converters". After his graduation in 2018, Stefan worked in the Austrian energy market on computational projects for the power and gas clearing. In 2021, he joined the Complexity Science Hub Vienna as a PhD Candidate and also the AIT as a Junior Scientist. Stefan's research interests center around data analysis and simulations. Since 2022, he is enrolled on the doctoral program of Computer Science at TU Wien. Currently, he works with Bernhard Haslhofer on crypto-asset analytics and published his first paper on Decentralized Finance (DeFi) compositions.

Friedhelm Victor obtained his PhD at TU Berlin, researching primarily on the intersections of blockchain, data science and privacy. Most of his works involve blockchain-based cryptoassets and the Ethereum network. More generally, he's interested in: Data Mining, Network Analysis, Privacy & Anonymity, and Fraud Detection. Prior to pursuing his PhD, he completed a Dual Master Degree in Computer Science at Technische Universität Berlin and at the Korean Advanced Institute of Science and Technology.

Pietro Saggese is a PostDoc Scientist at the Complexity Science Hub (CSH), in a joint program with the Austrian Institute of Technology (AIT), since May 2021. He obtained his Ph.D. at the Economics and Data Science department, IMT School for Advanced Studies in Lucca, Italy, in July 2021. In his current research at AIT and CSH, Pietro is focusing mainly on crypto asset analytics, and in particular on investigating the interplay between Decentralised Finance (DeFi) protocols deployed in Ethereum, to gain insights into the potential risks and opportunities associated with them. His research interests include cryptofinance, cryptoasset analytics, and their socio-economic implications.

Bernhard Haslhofer is a senior scientist at the Complexity Science Hub Vienna, where he leads the Cryptofinance research group. He is also a co-founder of Iknaio Cryptoasset Analytics GmbH. His general research interest lies in finding and applying quantitative methods to gain new insights from large-scale, connected datasets. Currently, he is mostly working on cryptoasset analytics, using quantitative approaches to answer various research questions related to cryptoassets. He also teaches a course on Cryptoasset Analytics at TU Vienna.

SUERF Publications

Find more **SUERF Policy Briefs** and **Policy Notes** at www.suerf.org/policynotes

SUERF is a network association of central bankers and regulators, academics, and practitioners in the financial sector. The focus of the association is on the analysis, discussion and understanding of financial markets and institutions, the monetary economy, the conduct of regulation, supervision and monetary policy.

SUERF's events and publications provide a unique European network for the analysis and discussion of these and related issues.

SUERF Policy Briefs (SPBs) serve to promote SUERF Members' economic views and research findings as well as economic policy-oriented analyses. They address topical issues and propose solutions to current economic and financial challenges. SPBs serve to increase the international visibility of SUERF Members' analyses and research.

The views expressed are those of the author(s) and not necessarily those of the institution(s) the author(s) is/are affiliated with.