University of Basel

Center for Innovative Finance

Decentralized Finance
On Composability and Wrapping Complexity

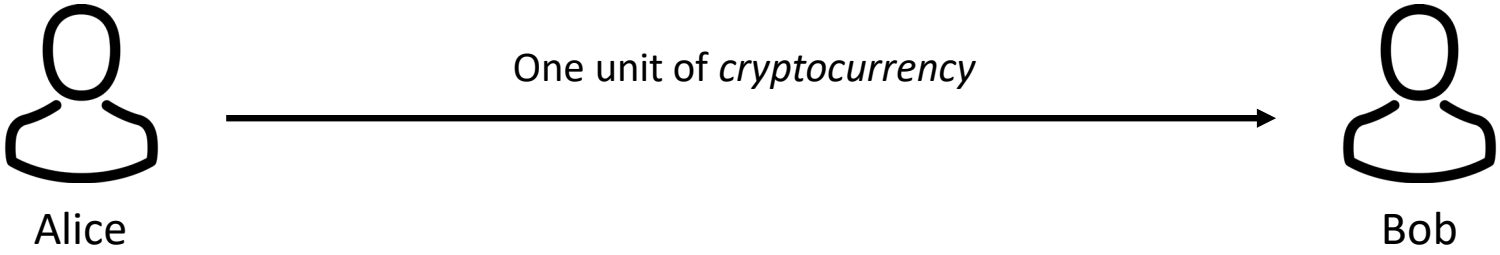
Prof. Dr. Fabian Schär

Faculty of Business and Economics, University of Basel

Educational purposes only. No investment advice. I am not a financial advisor.
Personal views only. Not necessarily in line with any organization I am affiliated with.
No official statements on behalf of any organization.

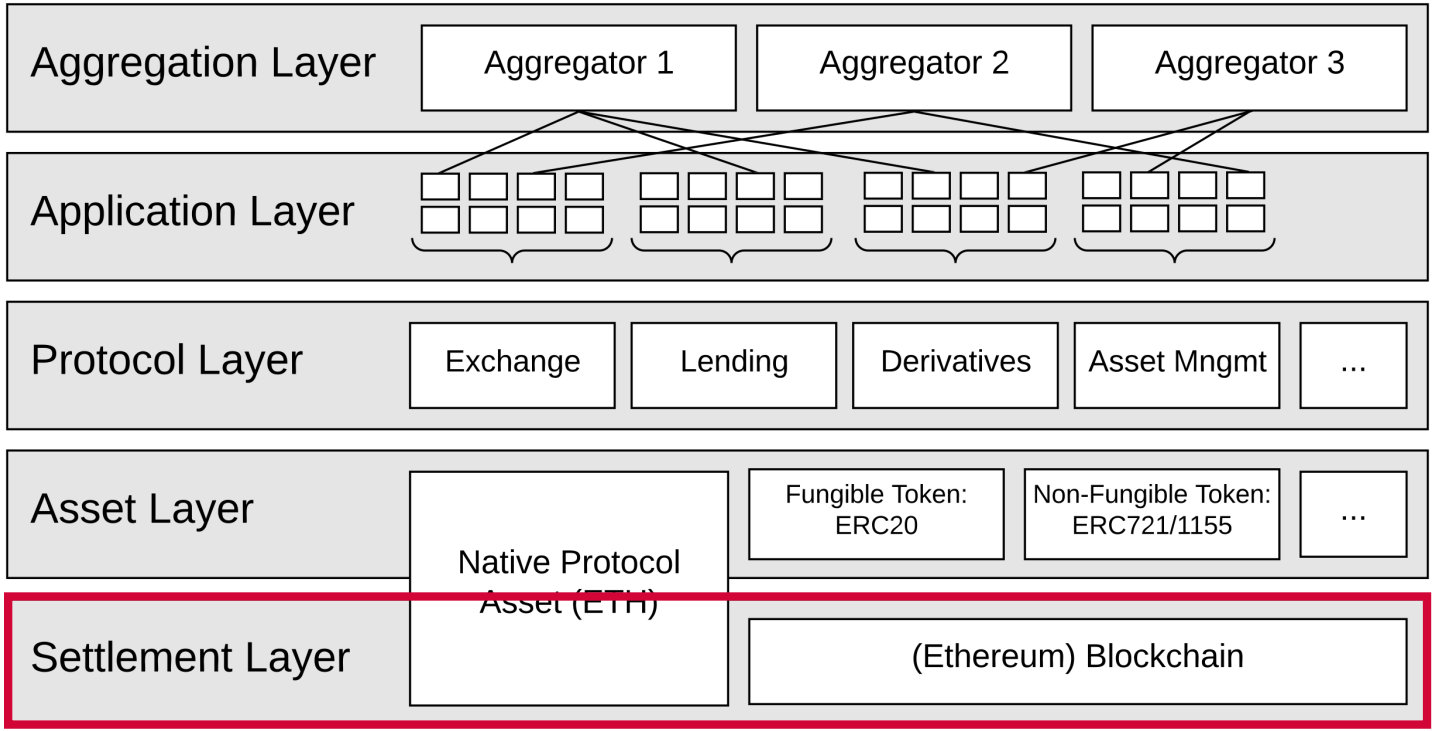
A Blockchain Transaction

What people usually have in mind:



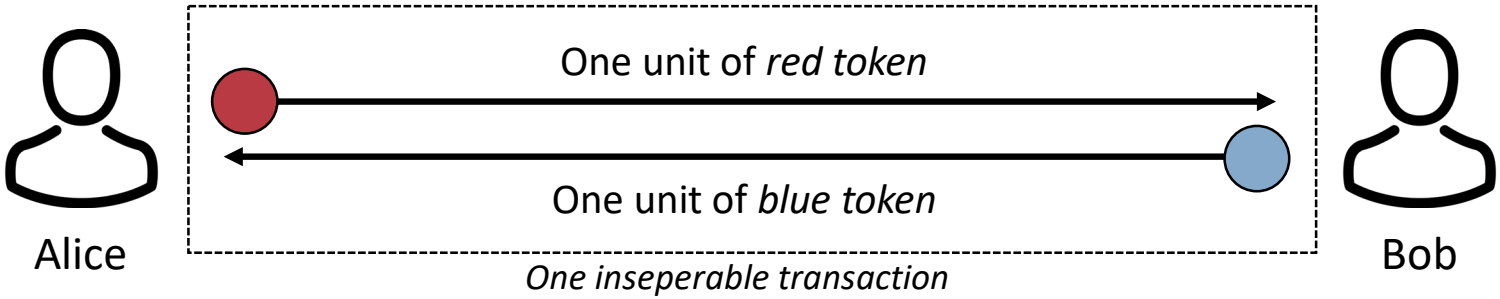
→ Ok… But what about some more exciting examples?

The DeFi Stack



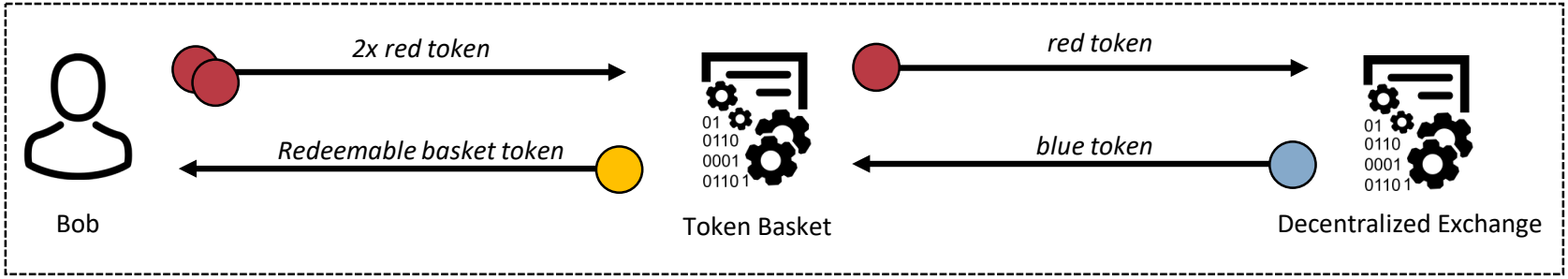
Schär (2021) Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets.

A Conditional Token Transaction



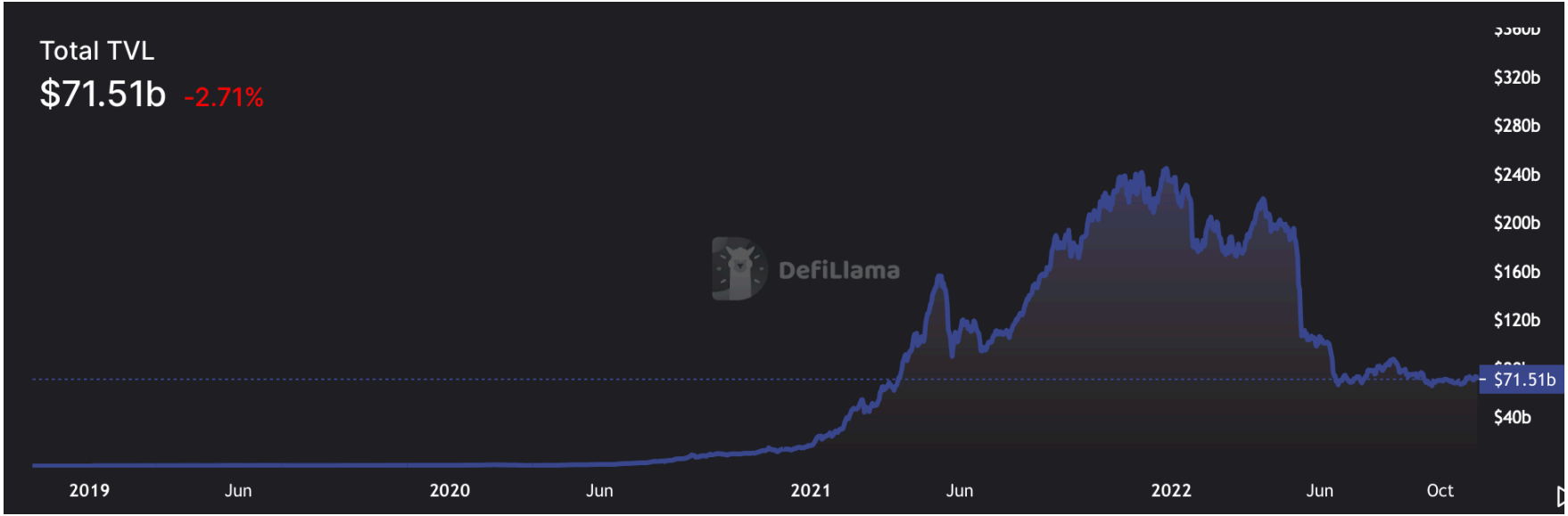
→ Atomicity and composability are very important concepts in DeFi.

Composability and Decentralization



In TVL We Trust… (You Should Not!)

Total value locked (TVL) is an inaccurate metric and (by itself) meaningless.



Source: DeFi Lama, November 7th 2022.

Potential for High Nesting Levels

Two Distinct Problems

1. **Wrapping Complexity**
2. **Intransparent Governance Token Allocation**

Nadler and Schär (2022)

Decentralized Finance, Centralized Ownership?
An Iterative Mapping Process to Measure
Protocol Token Distribution

Matthias Nadler
Center for Innovative Finance
Faculty of Business and Economics
University of Basel
Basel, Switzerland
matthias.nadler@unibas.ch

Fabian Schär
Center for Innovative Finance
Faculty of Business and Economics
University of Basel
Basel, Switzerland
f.schaer@unibas.ch

***Abstract*—In this paper, we analyze various Decentralized Finance (DeFi) protocols in terms of their token distributions. We propose an iterative mapping process that allows us to split aggregate token holdings from custodial and escrow contracts and assign them to their economic beneficiaries. This method accounts for liquidity-, lending-, and staking-pools, as well as token wrappers, and can be used to break down token holdings, even for high nesting levels. We compute individual address balances for several snapshots and analyze intertemporal distribution changes. In addition, we study reallocation and protocol usage data, and propose a proxy for measuring token dependencies and ecosystem integration. The paper offers new insights on DeFi interoperability as well as token ownership distribution and may serve as a foundation for further research.**

***Index Terms*—Blockchain Governance, Ethereum, Decentralized Finance, DeFi, Token Economy**

I. Introduction

Decentralized Finance (DeFi) refers to a composable and trust-minimized protocol stack that is built on public Blockchain networks and uses smart contracts to create a large variety of publicly accessible and interoperable financial services. In contrast to traditional financial infrastructure, these services are mostly non-custodial and can mitigate counterparty risk without the need for a centralized third party. Funds are locked in smart contracts and handled in accordance with predefined rules, as specified by the contract code. Some examples of DeFi protocols include constant function market makers, lending-platforms, prediction markets, on-chain investment funds, and synthetic assets, [1].

Most of these protocols issue corresponding tokens that represent some form of partial protocol ownership. Although the exact implementations, the feature sets, and the token holder rights vary greatly among these tokens, the reason for their existence can usually be traced back to two motives: *Protocol Governance* and *Protocol Economics*.

Governance: Tokens may entitle the holder to vote on contract upgrades or parameter changes. A token-based governance system allows for the implementation of new features. Moreover, the protocol can react to exogenous developments, upcoming interface changes, and potential bugs.

Economics: Most tokens have some form of implicit or explicit value-capture that allows the token holder to participate economically in the growth of the protocol. Value is usually distributed through a utility and burn mechanism (deflationary pressure) or some form of dividend-like payments. In many cases, initial token sales are used to fund protocol development and continuous release schedules to incentivize protocol usage.

Considering the two main reasons for the existence of these tokens, it becomes apparent that token distribution is a critical factor in the protocols' decentralization efforts. Heavily centralized token allocations may result in situations where a small set of super-users can unilaterally change the protocol – potentially at the expense of everyone else. Moreover, a heavily concentrated distribution may create an ecosystem where much of the value is captured by a small number of actors.

The authors are unaware of previous academic research on this subject. In August 2020, an analysis was circulated on social media, [2]. Simone Conti analyzed token contracts for their top holders and used this data to compute ownership concentration measures. However, the study was based on questionable assumptions and fails to account for the large variety of contract accounts. In particular, liquidity-, lending- and staking-pools, as well as token wrappers, had been counted as individual entities. As these contract accounts are mere custodians and usually hold significant token amounts on behalf of a large set of economic agents, this approach clearly leads to spurious results.

There are previous studies that tackle similar research questions in the context of the Bitcoin network, [3], [4], [5]. However, due to Bitcoin's relatively static nature and the separation of token ownership and protocol voting rights, the question is less pressing. Moreover, the fact that Bitcoin's standard client discourages address reuse makes these anal-

Algorithm 1 Iterative Mapping Process

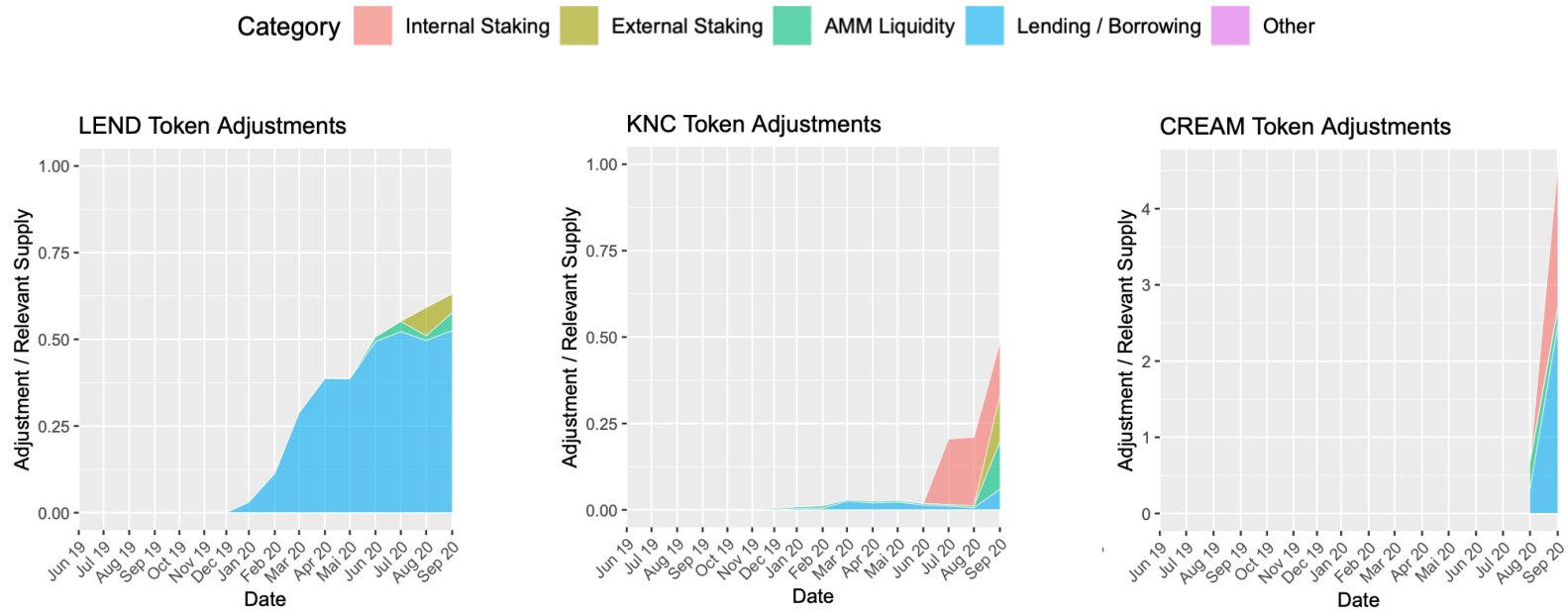
```
H ← initial token holder table
repeat
    sort H by token value, descending
    for all h ∈ top 1,000 rows of H do
        identify and categorize h
        apply inclusion logic to h
        if h is mappable then
            map h according to its category
        end if
    end for
until no mappable rows found in last iteration
assert every row with more than 0.1% of the total relevant
    supply is properly identified and categorized
```

Adjusted Ownership Table

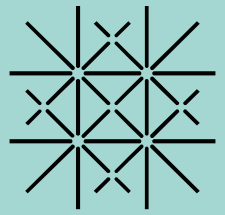
Token		Owner #	Top 5	Top 10	Top 50	Top 100	Top 500	Top 50%	Top 99%	Gini 500
LRC	Sep 20	66,382	13.75%	20.06%	43.44%	62.11%	87.9%	66	5,251	66.36%
	Trend	+1.49%	-2.3%	-1.68%	-1.26%	-1.14%	-0.41%	+3.23%	+7.95%	-0.74%
	σ 12m	3,392.5	0.0236	0.0232	0.0261	0.0313	0.0163	6.1	811.7	0.0205
MKR	Sep 20	29,765	24.43%	36.49%	67.71%	79.49%	93.72%	20	3,918	79.26%
	Trend	+8.31%	-3.45%	-2.12%	-0.45%	-0.19%	-0.12%	+4.5%	+7.17%	-0.22%
	σ 12m	4,511.7	0.0503	0.0405	0.0175	0.0107	0.0057	3.0	587.0	0.01
MTA†	Sep 20	5,595	13.81%	22.97%	51.18%	63.51%	88.27%	47	2,090	65.93%
NXM	Sep 20	7,355	32.17%	44.3%	70.42%	78.51%	91.29%	14	2,817	81.14%
	Trend	-36.69%	-2.87%	-2.71%	-1.65%	-1.12%	-0.37%	+18.09%	-33.11%	-0.24%
	σ 12m	1,918.2	0.0704	0.0992	0.0869	0.0619	0.0238	2.7	747.1	0.0434
REN	Sep 20	22,770	10.45%	15.29%	32.81%	41.79%	67.85%	166	8,500	55.31%
	Trend	+26.0%	-3.12%	-2.97%	-2.98%	-2.64%	-1.5%	+42.78%	+25.39%	-1.56%
	σ 12m	4,673.4	0.0232	0.0313	0.0671	0.072	0.0579	38.4	1,718.0	0.0437
SUSHI†	Sep 20	22,740	25.64%	35.26%	58.31%	66.28%	83.78%	28	7,300	74.11%
UMA†	Sep 20	5,634	56.21%	75.64%	96.87%	98.21%	99.43%	5	240	95.61%
YFI†	Sep 20	14,296	11.52%	16.98%	37.32%	48.1%	73.75%	114	5,145	57.6%
YFII†	Sep 20	8,513	20.8%	27.78%	53.93%	66.23%	85.15%	40	3,278	72.18%
ZRX	Sep 20	161,285	23.71%	38.4%	59.39%	63.87%	72.91%	21	38,404	82.63%
	Trend	+4.05%	-1.15%	-0.02%	+0.76%	+0.64%	+0.22%	-2.96%	+6.28%	+0.43%
	σ 12m	16,372.0	0.0133	0.0056	0.0158	0.0147	0.0082	3.6	5,233.6	0.0132

†Insufficient historical data.

The Dark Side of Composability



Source: Nadler and Schär (2021)



University
of Basel