European Securities and Markets Authority

ESMA webinar – TRV Risk Analysis articles on decentralised finance

Welcome remarks

Claudia Guagliano

ESMA, Head of Consumers, Sustainability and Innovation Analysis

Decentralised finance in the EU : Developments and risks

Anne Chone, ESMA

Why consider DeFi now?

ESMA

11 October 2023
[illegible]

ESMA TRV Risk Analysis

Financial Innovation

Decentralised Finance: A categorisation of smart contracts

ESMA

11 October 2023
ESMA50-2085271018-3349

ESMA TRV Risk Analysis

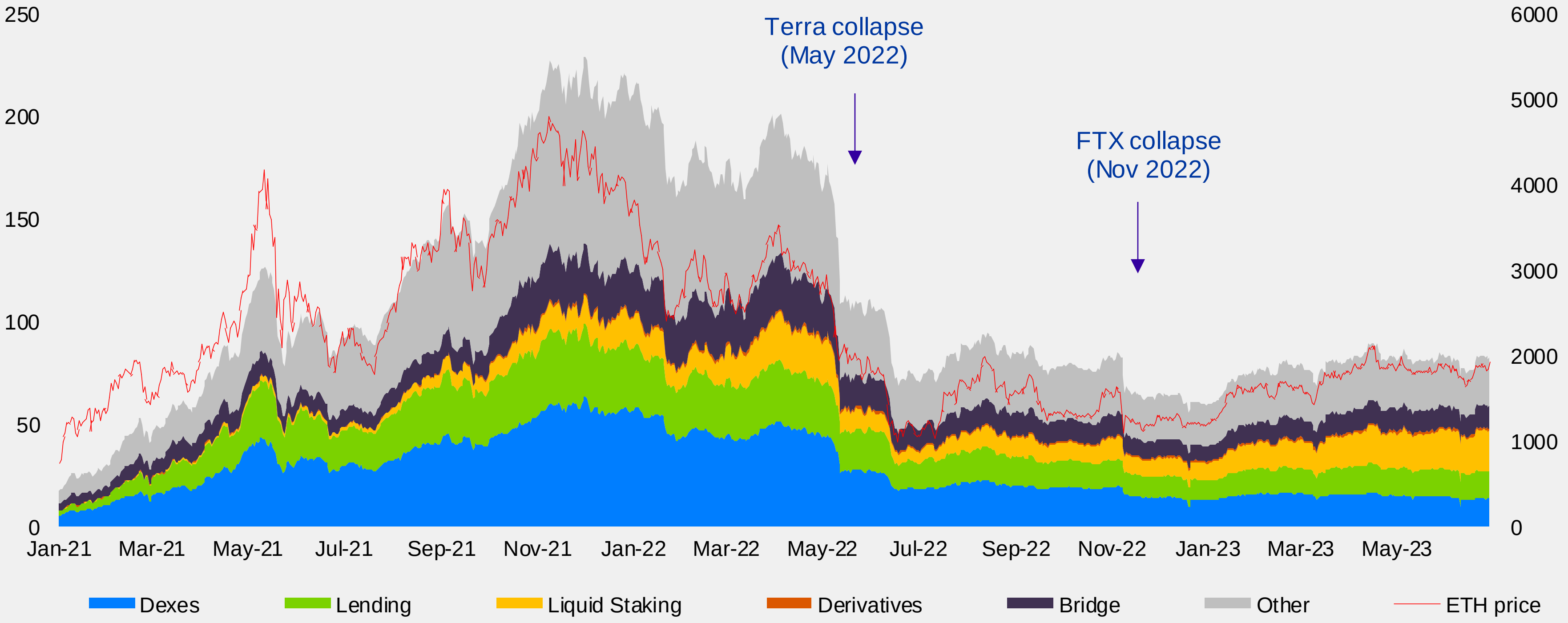
Financial Innovation

Decentralised Finance in the EU: Developments and risks

- Latest and arguably most innovative development in crypto area
- Expanding number of applications and users
- Complex and opaque structures
- Not directly addressed by newly introduced markets in crypto-assets regulation (MiCA)

Assess risks to ESMA's objectives and inform MiCA's future review

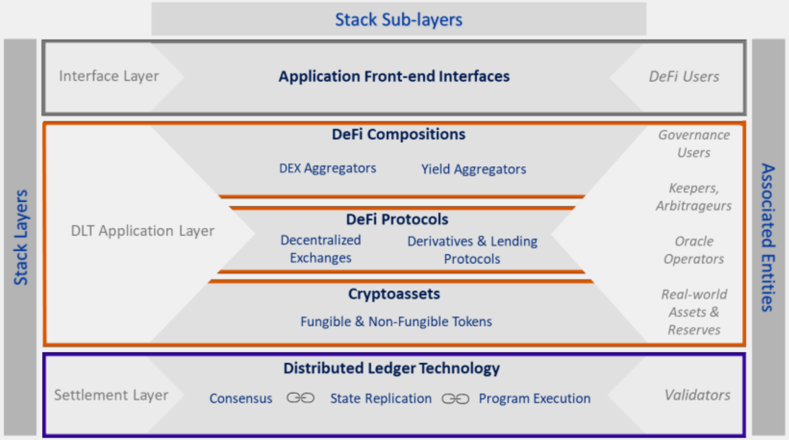
DeFi development: a roller coaster ride



+2,800 DeFi protocols but three largest represent 30% of TVL

DeFi’s distinguishing features

- The DeFi ‘stack’
- Decentralisation
- Stablecoins, oracles and bridges



Stack Sub-layers

Stack Layers

Associated Entities

Interface Layer — Application Front-end Interfaces — *DeFi Users*

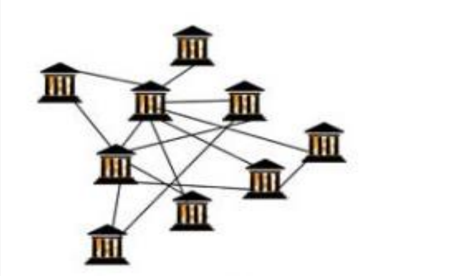
DLT Application Layer

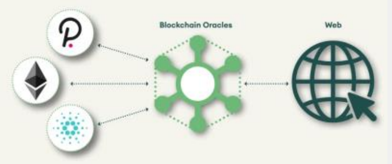
DeFi Compositions: DEX Aggregators, Yield Aggregators — *Governance Users*; *Keepers, Arbitrageurs*

DeFi Protocols: Decentralized Exchanges, Derivatives & Lending Protocols — *Oracle Operators*

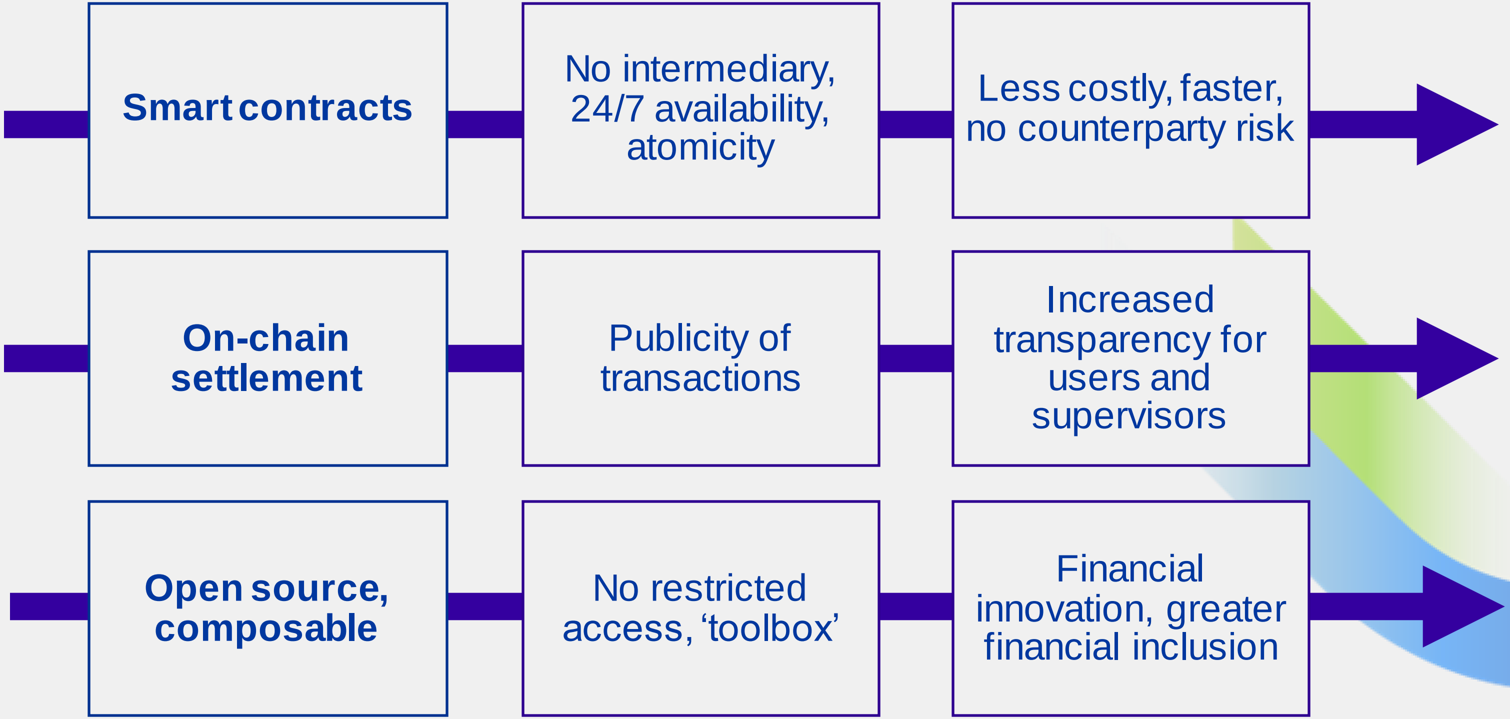
Cryptoassets: Fungible & Non-Fungible Tokens — *Real-world Assets & Reserves*

Settlement Layer — Distributed Ledger Technology: Consensus, State Replication, Program Execution — *Validators*





Some potential benefits, still to be confirmed



Smart contracts → No intermediary, 24/7 availability, atomicity → Less costly, faster, no counterparty risk

On-chain settlement → Publicity of transactions → Increased transparency for users and supervisors

Open source, composable → No restricted access, 'toolbox' → Financial innovation, greater financial inclusion

Important risks to DeFi users

Risks inherent to traditional finance	Market risk	Liquidity risk	Counterparty risk
Features of underlying assets & products	Many crypto-assets highly speculative	Elevated leverage	Collateralization, but…
Features of underlying technology	Open source	Disintermediated access, no KYC	Composability, autonomous smart contracts

Risks to consumer protection

No material risks to financial stability yet

- Same vulnerabilities sources as traditional finance
  - Liquidity and maturity mismatch
  - Leverage
  - Interconnectedness
- But still very small in size
- Limited risk contagion channels between DeFi and traditional markets
- But requires monitoring

Crypto transactions: DEXs address certain pain points

	CEXs	Order-book DEXs	Automated Market Makers DEXs
Order book	Off-chain	Off-chain	On-chain
Pricing mechanism	Same as traditional exchanges	Same as traditional exchanges	Pre-set 'conservation' function, e.g., constant product function
Settlement	Off-chain + (at periodic intervals) on-chain	On-chain	On-chain
Custody of clients assets	Yes	No	No

Central point of failure, misappropriation of client assets, conflicts of interest

↔

Lack of clearly identified responsible party, congestion, MEV

New vulnerabilities sources and manipulation techniques

ESMA
European Securities and Markets Authority

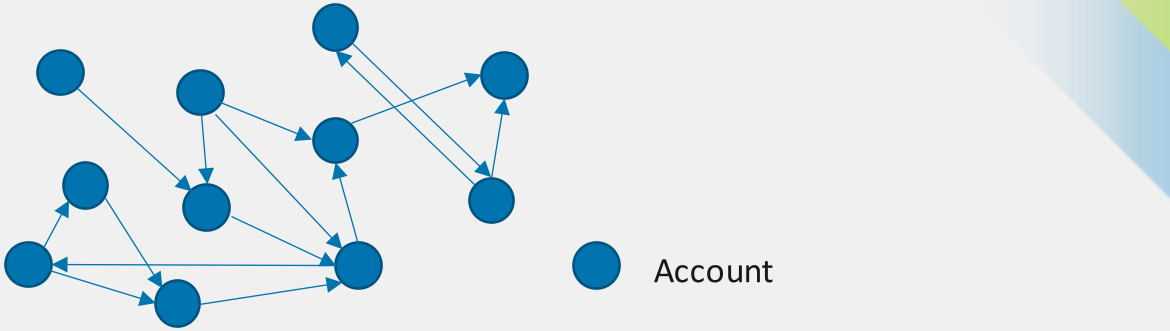
		Crypto / DEXs unique features	Scope of the phenomenon
Wash trading	🔴	Speculative assets, concentrated ownership	• 77.5% of traded volumes on unregulated exchanges on average • 30% of crypto-assets victim of wash trading on order-book DEXs
	🟢	Publicity	
	🔴	Pseudonymity	
	🔴	Cost-free account creation	
Pump & dump schemes	🔴	Speculative assets, concentrated ownership	• Thousands of online chat rooms dedicated to pump & dump schemes • Up to USD 120bn in annual crypto volumes
	🟡	Social media, deep and dark web	
	🔴	Limited financial literacy	
	🔴	Flash loans	
	🔴	Oracles	
Front-running (back-running and sandwich attacks)	🟡	Publicity (mempool)	• USD 550-650mn Maximal Extractable Value on largest Ethereum based protocols between 2020 and 2022 • USD 100mn losses from front-running attacks from May 2020 to April 2021
	🔴	Consensus mechanism	
	🔴	Flash loans	
	🔴	Oracles	

A categorisation of smart contracts

Zeno Benetti, ESMA

Blockchains as (directed) networks

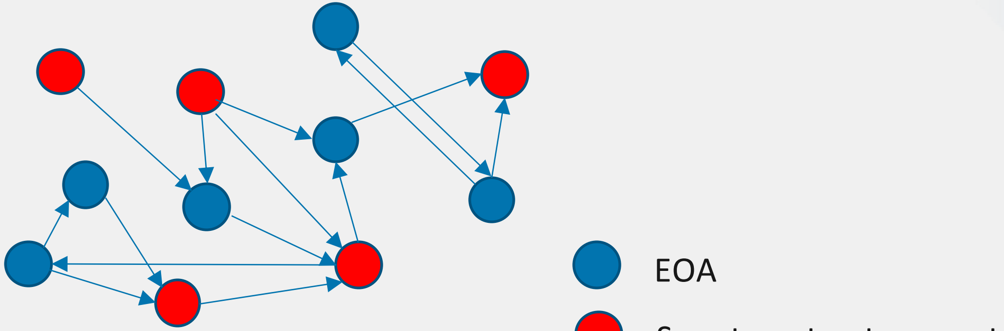
- An ‘account’ on a blockchain is an entity with a cryptocurrency balance that can send transactions (to other accounts)
- Thus, a blockchain can be viewed as a network of nodes and edges, where nodes are the ‘accounts’ and edges are the ‘interactions’ (the transactions) among said accounts



Blockchains as (directed) networks

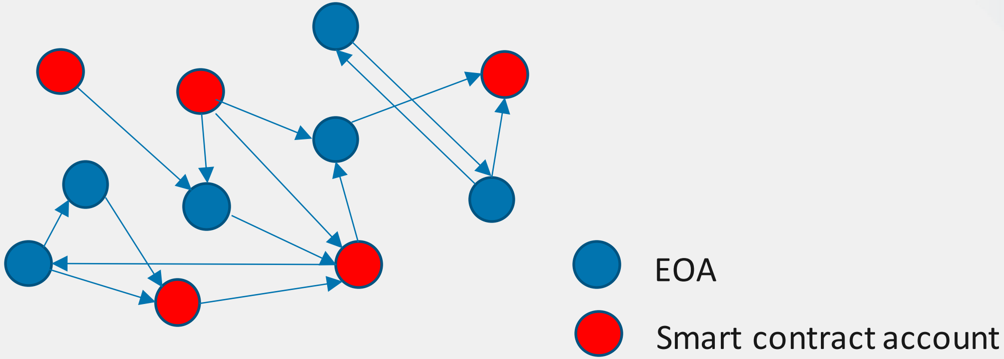
On Ethereum, there exists two types of accounts:

- Externally-owned accounts (EOAs)
- Smart contract accounts



Blockchains as (directed) networks

- Just as EOAs, smart contract have a balance and can be both the sender and the target of a transaction
- Yet, smart contract are not controlled by a user. Instead, their actions are defined by a code written in a programming language (the **‘source code’**).
  - ➢ Smart contracts are computer programs that live on the blockchain and execute automatically, interacting with other accounts on the blockchain (be they EOAs or other smart contracts) according to the code that defines their actions



Defining smart contracts

- Szabo (1997) defines a smart contract as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises”.*
- Four fundamental properties can be derived from this definition:

➢ ***A set of promises***: Smart contracts consist of contractual terms and/or rules-based operations designed to carry out an economic activity.

➢ ***Specified in digital form***: Smart contracts are concluded and enforced digitally, and consist of lines of code within software that execute predetermined rules when a condition is met.

➢ ***Protocols***: The set of code-based rules and the data are processed by an algorithm (or a combination of algorithms).

➢ ***Within which the parties perform***: The execution of the contract is immutable.**

* Szabo, N. (1997). *Formalizing and Securing Relationships on Public Networks.*

** Antonopolous, A. (2018). *Mastering Ethereum: Building Smart Contracts and dApps.*

Risks inherent to smart contracts

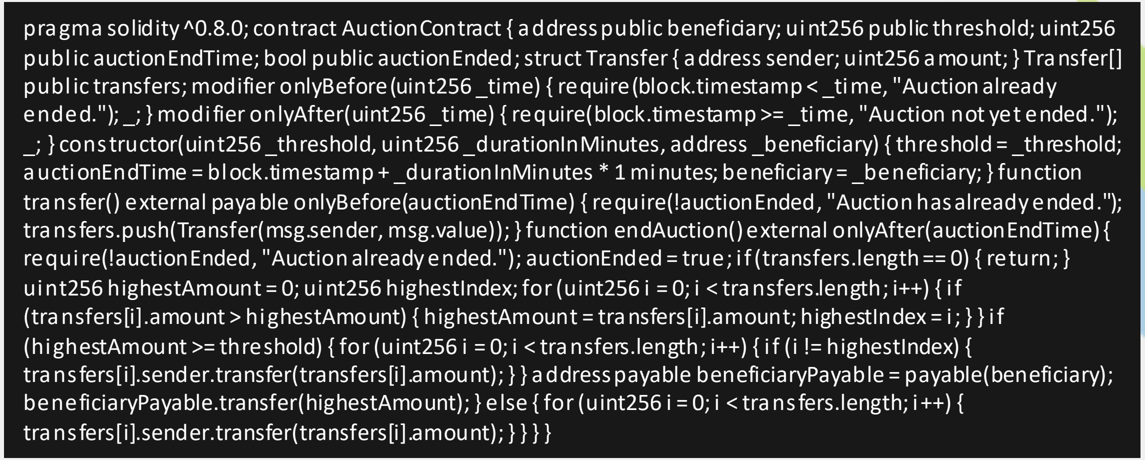
- Risks to users:
  - inability to modify or terminate smart contracts
  - the transaction-ordering dependency vulnerability
  - the timestamp dependency vulnerability
  - the mishandled exception vulnerability
  - trustworthiness of data feeds ‘oracles’
  - ‘illicit’ smart contracts
- Risks to financial stability:
  - composability and consequent propagation risk
  - unregulated rehypothecation
  - concentration risk on key nodes

Topic modelling on smart contracts

- Topic modelling is the task of **discovering latent topics (themes) within a given corpus of documents**:
- It relies on three fundamental assumptions:
  - ➢ Each **topic is defined as a distribution of words**
  - ➢ Each **document is a mixture of topics**
  - ➢ Within each document, **each word is drawn from a topic**

Feeding smart contracts to a topic model

- Smart contracts **source code is essentially a long string** (such as the one below for the mock smart contract seen before)
- As such, it can be fed into a topic model, which in our case is the **Latent Dirichlet Allocation (LDA)**

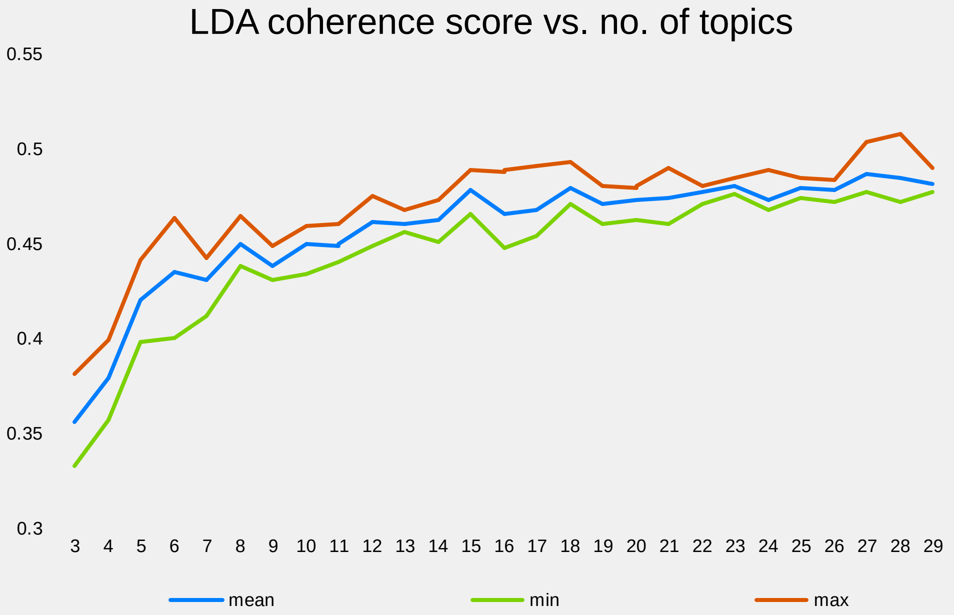


```
pragma solidity ^0.8.0; contract AuctionContract { address public beneficiary; uint256 public threshold; uint256
public auctionEndTime; bool public auctionEnded; struct Transfer { address sender; uint256 amount; } Transfer[]
public transfers; modifier onlyBefore(uint256 _time) { require(block.timestamp < _time, "Auction already
ended."); _; } modifier onlyAfter(uint256 _time) { require(block.timestamp >= _time, "Auction not yet ended.");
_; } constructor(uint256 _threshold, uint256 _durationInMinutes, address _beneficiary) { threshold = _threshold;
auctionEndTime = block.timestamp + _durationInMinutes * 1 minutes; beneficiary = _beneficiary; } function
transfer() external payable onlyBefore(auctionEndTime) { require(!auctionEnded, "Auction has already ended.");
transfers.push(Transfer(msg.sender, msg.value)); } function endAuction() external onlyAfter(auctionEndTime) {
require(!auctionEnded, "Auction already ended."); auctionEnded = true; if (transfers.length == 0) { return; }
uint256 highestAmount = 0; uint256 highestIndex; for (uint256 i = 0; i < transfers.length; i++) { if
(transfers[i].amount > highestAmount) { highestAmount = transfers[i].amount; highestIndex = i; } } if
(highestAmount >= threshold) { for (uint256 i = 0; i < transfers.length; i++) { if (i != highestIndex) {
transfers[i].sender.transfer(transfers[i].amount); } } address payable beneficiaryPayable = payable(beneficiary);
beneficiaryPayable.transfer(highestAmount); } else { for (uint256 i = 0; i < transfers.length; i++) {
transfers[i].sender.transfer(transfers[i].amount); } } } }
```

Feeding smart contracts to a topic model

- We applied a Latent Dirichlet Allocation (LDA) to our sample of smart contracts (~300.000 verified smart contracts).
- The performance of an LDA can be estimated via the **‘coherence score’**.
- The coherence score ranges from 0 to 1. The closer it is to 1, the higher the inter-topic heterogeneity and the intra-topic homogeneity.

Findings



Note: y-axis: Coherence score of the LDA model applied to 10 subsets (no replacement) of our set of smart contracts; x-axis: number of topics yielded by the LDA model
Source: ESMA

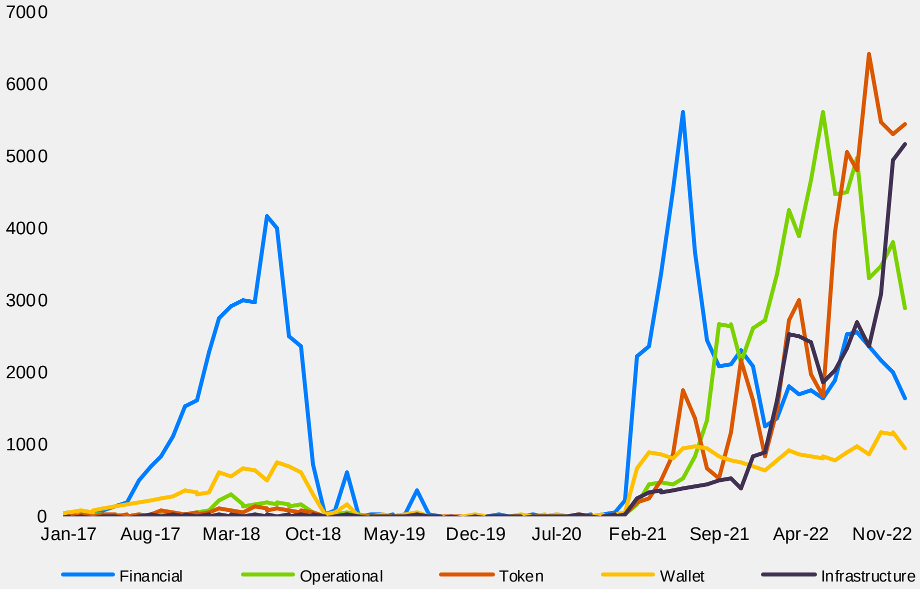
Findings

- Given that that of topic modelling is an unsupervised task, we need to label topics manually based on either
  - ➢ the terms that characterise them
  - ➢ the features of the contracts comprised therein

- Sticking with five topics, we defined assigned the following labels:
  - ➢ ***Financial***
  - ➢ ***Operational***
  - ➢ ***Tokens***
  - ➢ ***Wallets***
  - ➢ ***Infrastructure***

Findings

Incidence in the deployment of each category (2017 - 2022)



Note: Monthly smart contracts deployment per category of contract
Sources: ESMA

Conclusion

In our article, we show that application of topic modelling (LDA) on the source code of smart contracts can yield tools that:

- are **robust to changes in the dataset**,
- can potentially be **applied on a smart contract as of the moment of its deployment** on the blockchain (that is, before other nodes on the blockchain network start interacting with it),
- can **contribute to an enhanced and nuanced understanding of DeFi**, as well as to **identifying related significant risks**.

DECENTRALISED FINANCE IN THE EU

Discussion points on ESMA Papers:
- Developments and Risks
- A categorisation of smart contracts

Iota Kaousar Nassr
Capital Markets and Financial Institutions
OECD Directorate for Financial and Enterprise Affairs

ESMA Webinar
25 October 2023

OCDE
DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

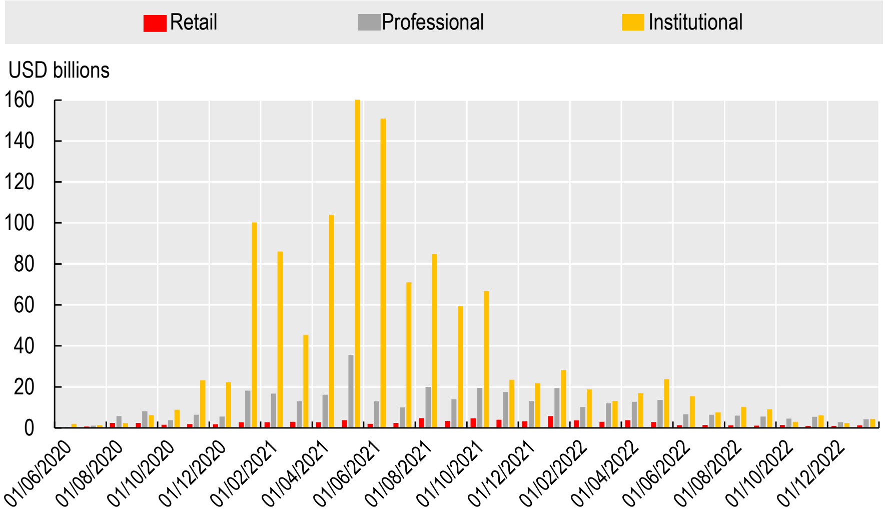
Discussion points

- DeFi risks and focus on retail investors
- The importance of continuous monitoring of emerging risks and for international collaboration
- Still, not all is bleak
  - Smart contracts

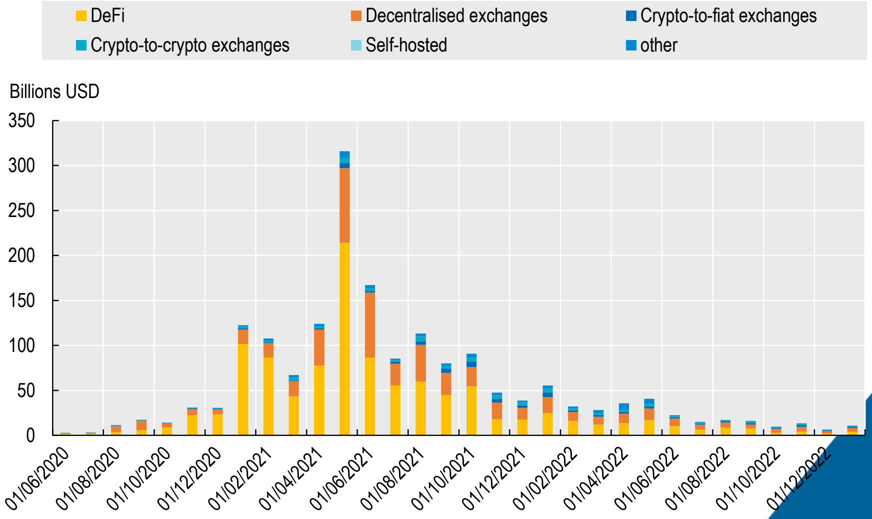
DeFi has been a professional investor play thus far

- **Professionals and institutionals dominate DeFi protocol activity globally in any given month**
- More than half of fund inflows to DeFi come from DeFi in any given month (leverage)

Negligible minority of DeFi transactions come from retail investors (below USD 10K)



Inflow of funds to DeFi by type of investor

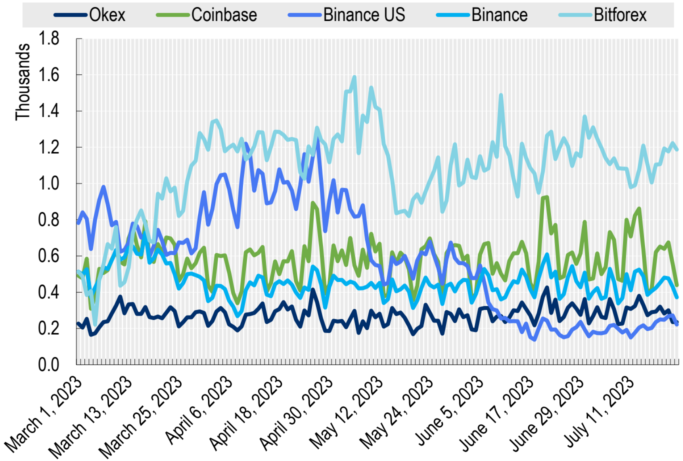


Source: (OECD, 2022) Why DeFi matters and the policy implications; (OECD, 2022) The institutionalisation of crypto-assets and DeFi-TradFi interconnectedness.
Note: Institutional transactions representing those above USD1 m, professional between USD10K and USD 1 m, retail representing those below USD 10K. Crypto-to-crypto exchanges are venues for the trading of cryptocurrencies primarily for other cryptocurrencies, either via a central limit order book or peer-to-peer via a centralised escrow. Crypto-to-fiat exchanges are venues for the trading of cryptocurrencies primarily for fiat, either via a central limit order book or peer-to-peer via a centralised escrow. Source: OECD based on Chainalysis data as of 31 July 2023.

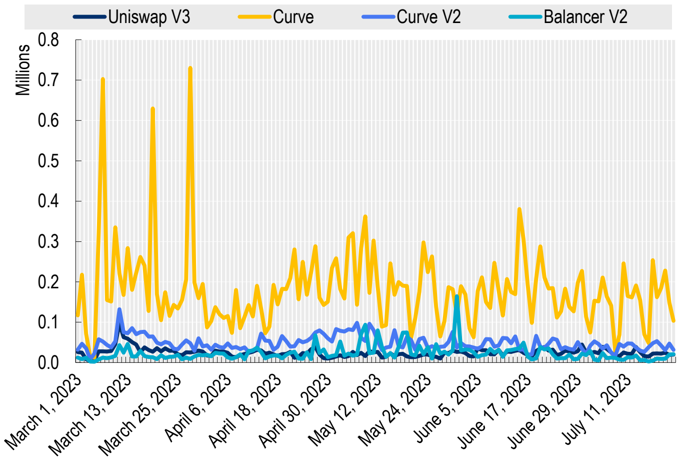
Similar trends observed at crypto-exchange trading

- **Particularly evident in decentralised exchanges**
  - **Average trade size on DEXs is 10x – 100x higher than the average trade size on CEXs**
  - Particularly in the case of stablecoin trading
- Differences could also be attributed to structural differences

Average trade size at centralised crypto-exchanges (CEXs) (in USD thousands)



Average trade size at decentralised crypto-exchanges (DEXs) (in USD millions)



Source: (OECD, forthcoming) The limits of DeFi for financial inclusion: lessons from ASEAN. Calculations based on Kaiko data as of 31 July 2023.

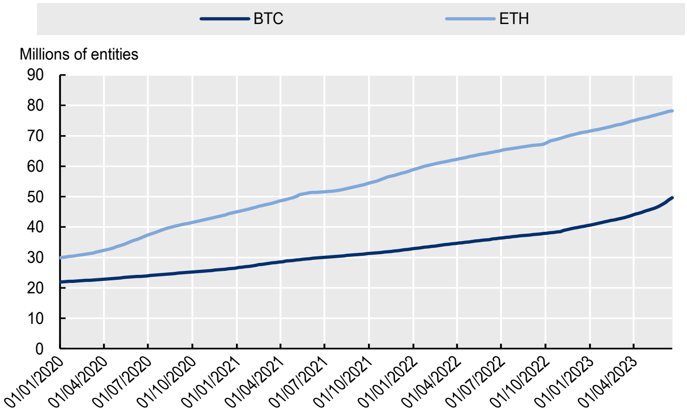
Yet, global retail crypto-activity is growing

- Despite prominence of professionals, **retail participation in wider crypto-asset markets is growing**
  - Retail investors disproportionately affected from crypto-winter (net buyers against larger wallets offloading crypto)

- Arguably, DeFi could be considered outright **unsuitable for retail investors**
  - Complexity, non-custodial nature, digital skills required, elaborate trading strategies involved

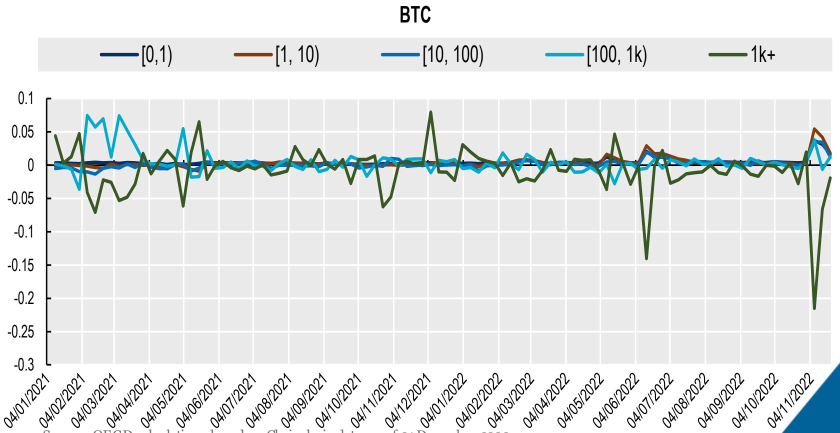
- Importance of protecting retail investors against risks emerging from DeFi

Addresses holding a maximum of 1 Bitcoin / 10 Ether



Source: (OECD, forthcoming) The limits of DeFi for financial inclusion: lessons from ASEAN. Calculations based on Chainalysis data, as of 31 July 2023.

Small crypto-holders net buyers in the aftermath of the crypto-winter



Source: OECD calculations based on Chainalysis data, as of 01 December 2022.

Importance of keeping an eye on DeFi emerging risks

ESMA paper provides a comprehensive analysis of risks involved in DeFi activity. There is merit in continuous monitoring of DeFi markets and emerging risks, such as the one provided in the ESMA report.

- Example: Today, limited interconnectedness DeFi – TradFi
  - However, developments in decentralised finance and DLT-based finance could change that in the future

Tokenisation example

- Limited development thus far
  - Limited incentives in highly efficient markets; legal framework limitations (e.g. ownership); liquidity; economics
  - And, until now absence of tokenised form of fiat for payment leg

- Potential implications of a scenario of **proliferation of tokenisation** and possible future links to DeFi
  - **e.g. scenario of use of tokenised assets instead of crypto-assets on DeFi**

=> Scenario analysis points to the importance of continuous monitoring of DeFi markets, their evolution and emerging risks

⇒**Importance of international coordination, consistency, capacity**

Still, not all is bleak: DeFi benefits and smart contracts

- There is merit in examining potential **benefits** of DeFi:
  - What can we learn from DeFi to **capture potential efficiencies** and allow for **productivity gains in financial market infrastructure**?
- Concepts of (compliant) DeFi for TradFi
  - **Smart contracts** and automation / Atomic settlement and post-trade / Programmability, encryption / AMMs to crowdsource liquidity (Pj Marianna)

ESMA's smart contract categorisation results

- Provides evidence of continued interest in DLT-based activity
  - Noteworthy increase in the number of deployed contracts in spite of market downturn
  - Spikes in **"finance"** category mapping the high **volatility** of this market
- **"Tokens"** category remains important while "finance" declines
  - Could that indicate utility tokens usage? Coupled with increasing importance of **"infrastructure"** category
  - Non-financial applications of ETH-based DLT activity (identity and logins; social media; supply chains..)
- Related, rising occurrence of **"wallet"** in the ESMA study: Shift towards smart-contract-based wallets in Ethereum

Questions remain

- Is total **transparency** of smart contract code welcome in financial use cases?
- Would **audits** of code of smart contract help promote trust?

Thank you!

iota.nassr@oecd.org

www.oecd.org/finance

OCDE

DES POLITIQUES MEILLEURES
POUR UNE VIE MEILLEURE

Q&A session

ESMA

European Securities and Markets Authority

ESMA webinar – TRV Risk Analysis articles on decentralised finance