EUROPEAN BLOCKCHAIN ASSOCIATION

Unstoppable Finance

大成 DENTONS

Regulating Decentralized Finance

An approach for Europe

Designed by fullvektor/freepik

Erwin Voloder has been involved in the blockchain sector since 2017, first as a start-up founder in Canada and currently as a regulatory and technical expert in Europe. He is a former economist with both the European Commission and European Central Bank. Currently he is Senior Policy Fellow at the European Blockchain Association. He frequently participates in working groups on programmable money and decentralized finance both at EU level and internationally including advising both private sector companies and national governments on both crypto regulation and blockchain based industrial solutions. His areas of expertise include tokenization, monetary policy, regulation, geopolitics and programmable money. His current line of research focuses on programmable money solutions for cross-border payments, and the development of 'digital currency areas' involving both CBDCs and stablecoins in geopolitical context.

Eugenio Reggianini is a cross industry professional with a solid background in corporate development, legal and strategy-consulting advisory for investments, product management and software architecture with working experience in Europe and Asia. Starting as Lead in DLT communities (Hyperledger - R3) with past involvement in projects related to Consortium corporate formation, product business development. Today, he is advising financial institutions, technology providers and enterprises along their digital transformation journey in adopting Blockchain and distributed ledger technologies by achieving short, medium and long term business objectives. He also represents the European Blockchain Association as Ambassador for Asia Pacific, serves as an expert member of the European Blockchain Observatory & Forum as well as part of Swiss Crypto and Digital Euro Association(s).

Peter Grosskopf is Co-Founder and CTO at Unstoppable Finance GmbH a Berlin based company with the mission to empower people around the world to access, interact with and unlock financial opportunities of the decentralized economy by building Ultimate.money. Before he was CTO and MD at Börse Stuttgart Digital Exchange, the first regulated digital asset exchange in Germany. Before he was CTO and co-founder at solarisBank. Peter has a technology and entrepreneurial background. In 2008 he founded a software engineering consultancy with focus on digitization projects and grew it to profitability to 30 employees. In 2014 he came to Berlin to join the company builder Hitfoxgroup and Finleap that focuses on fintech as CTO. Blockchain and decentralization fascinates him from the moment he got in touch at the end of 2016. Since then he has shaped the vision to bring decentralized finance to reality

Hagen Weiss is a Counsel in the Corporate and M&A practice at global law firm Dentons. Based in Frankfurt, he advises both regulated financial institutions and other companies on digital finance, DLT and Blockchain, the German Electronic Securities Act (eWpG), the Markets in Crypto Assets Regulation MiCA, and the EU-DLT Pilot Regime. He also advises clients on financial sanctions and dispute resolution. By drafting many of the pertinent legal statutes as a regulator and policy maker, Hagen Weiss has been a significant contributor to the regulatory and legal framework for crypto assets at the German, European, and international level. Having previously worked for Federal Agencies and the German Federal Ministry of Finance, he has extensive knowledge in the area of regulatory decision-making.

EXECUTIVE SUMMARY

2022 has seen a spate of market failures in the cryptoasset space, largely driven by poor risk management, commingling of funds, excessive leverage, a lack of consistently and appropriately applied regulation, rehypothecation and hubris. These negative outcomes were dominated by centralized crypto (CeFi). Where centralized exchanges and lenders – crypto's de facto 'banks' have failed to protect investors, the same outcomes have not carried over into decentralized finance (DeFi). In fact, decentralized exchanges (DEXs) are non-custodial by design, with asset swaps and liquidity allocation conducted P2P while relying on code and protocols rather than central limit order books or routing.

DeFi relates to the public-blockchain based financial infrastructure orchestrated through the use of smart contracts which has been able to replicate a variety of different financial services. Through smart contracts, these financial services become more composable (the lego block analogy), interoperable, transparent and avoid the need for third parties. However DeFi is not infallible, and as the market continues to grow – drawing in both attention and capital – the challenges with how best to regulate the sector will grow with it. Pseudonimity and lack of formal leadership structures may create systemic instabilities and hinder long-term adoption as well as prevent bringing to bear DeFi's proven advantages to financial markets.

Recently, the European Commission Directorate-General for Financial Stability, Financial Services and Capital Markets Union (FISMA) released a consultation paper '*Decentralized Finance: information frictions and public policies, approaching the regulation and supervision of decentralized finance*.' The paper takes a broad view at identifying points of friction that are unique to DeFi, how these frictions relate to both its competitive advantage but also potential drawbacks in the long run, and what role the public sector can play to continue fostering innovation while creating a level playing field.

Erwin Voloder and Eugenio Reggianini from the European Blockchain Association, together with Peter Grosskopf from Unstoppable Finance and Dentons' Hagen Weiss have published an industry response to the policy proposals espoused in the Commission's consultation paper. It is our shared view that a responsible role for regulators is both necessary and encouraged if DeFi is to develop long term viability beyond the hype cycles emblematic of crypto's current peaks and troughs. That being said, the fallout from recent shakeups in the cryptosphere has also catalyzed a heavy handed tone from the official sector both in Europe and abroad as to how best to ring fence the use of blockchain in financial markets. With the coming of the Markets in Crypto Assets Regulation (MiCA), Europe is already leading in setting a standard regarding public policy. It is our hope that this reply serves as the foundation for a concrete discussion on how best to regulate DeFi in a way where the public and private sectors can each fall back on their comparative advantages while innovation is allowed to continue safely and unencumbered.

I. TradFi Information asymmetries

In traditional financial markets everyone seeks optimal trading and risk allocations. The point when interactions between agents begin to exhibit frictions in their transaction technology, an optimal outcome is no longer possible. Diamond (1984) shows that information frictions may prompt investors to lend to intermediaries who then lend to borrowers because they lack information on a downstream borrowers incoming cash flows. Technological investment is needed to overcome such asymmetries and associated deadweight loss. Bank-client relationships have also traditionally been used to overcome incomplete knowledge of proprietary information between contracting parties. As such, regulating and supervising financial intermediation has traditionally revolved around a set of rules which seek to both guide and instruct the behavior of financial intermediaries. Examples include rules for Anti-Money-Laundering/Counter-Terrorist Financing (AML/CTF), liquidity coverage ratios and know-your-customer/business (KYC/KYB) rules. Regulation allocates the safekeeping of private information and use of verification/monitoring technologies to financial intermediaries. Disclosure of this private information is expressly forbade without prior client consent.

II. DeFi Information Asymmetries

Smart contracts only need publicly verifiable and accessible information at the time of execution to instantiate a financial product or service. The use of pseudonymity and on-chain transparency lets DeFi markets efficiently allocate liquidity and issue novel products such as flash loans, or other forms of lending. For example an automated market maker (AMM) will connect two agents directly through a liquidity pool while an algorithm prices assets instead of using the information from buy/sell orders in limit order books. The combination of incomplete verification information and ledger transparency makes decentralized finance directly bounded to the information structures that are possible through smart contracts.

III. Taxonomy of DeFi protocols

In order to create a path to understanding the concept frameowrk architecture (below), we rely here on the original paper's classification of DeFi protocols:

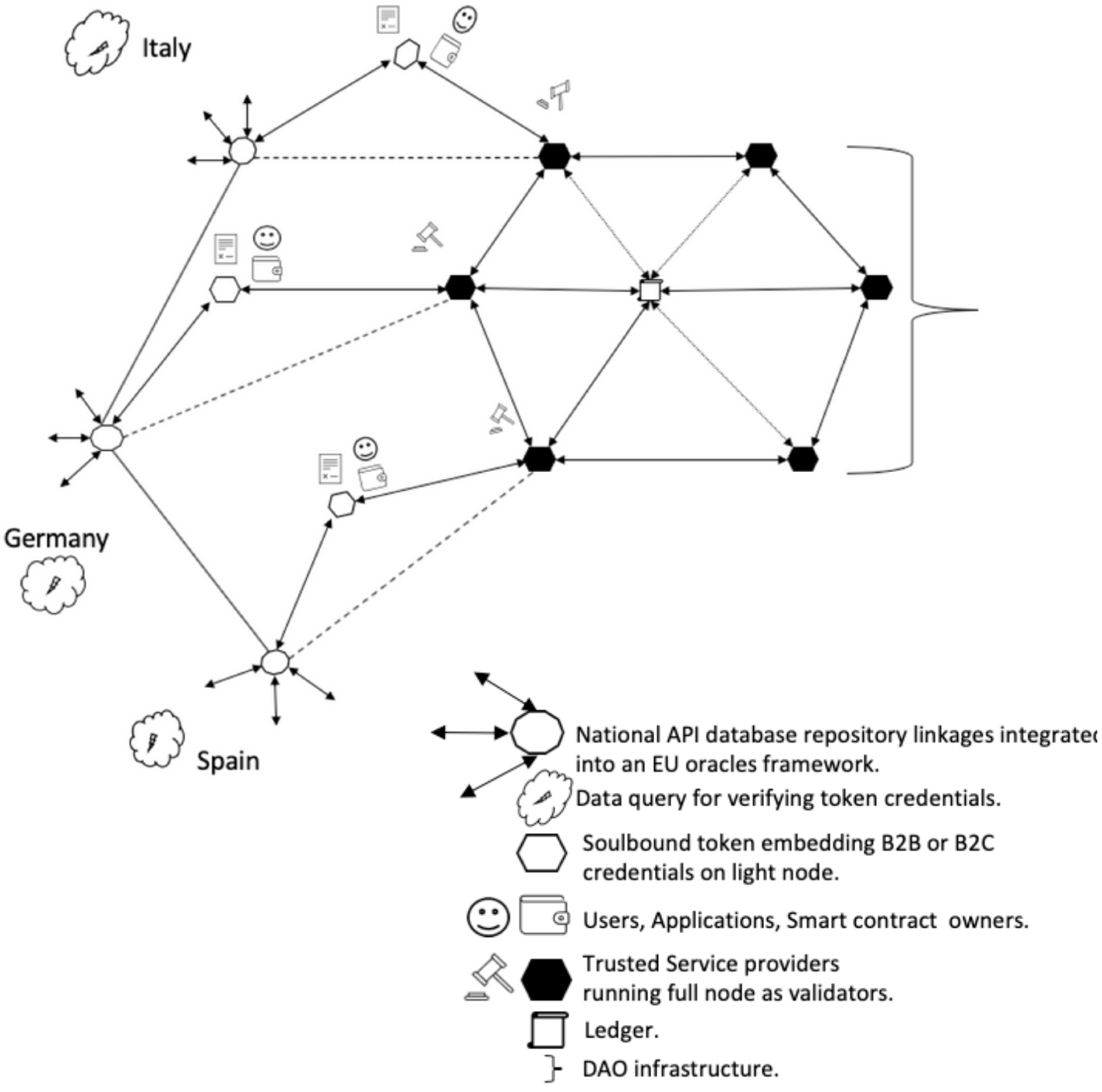
Autarkic: Internally consistent protocols which rely strictly on information produced under their own activity, which is therefore fully verifiable.

Crossing: Increasing underlyingly verifiable information achieved when a protocol crosses information with other protocols, e.g. through shared ledgers.

Off-chain: information assessed by the protocol is both publicly verifiable, alongside information submitted via external providers (e.g. oracles), whose input cannot be formally verified by the ledger.

Based on the classification criteria we have devised a European-based conceptual model for how information asymmetries in decentralized markets may be overcome in such case where both public/private sector entities are optimized to capitalize on their comparative advantages. A discussion of the process flow and policy implications follows. In that context a public DAO infrastructure interacts with private application owners and related users leveraging so called “SoulBound” tokenization processes and public oracles to minimize the asymmetry information risk into a regulatory flexible and innovative environment.

Figure 1. Overcoming information asymmetries in DeFi markets through DAO infrastructure, Soulbound Tokens (SBTs) and national API’s via EU oracle frameworks.



The outline model in Figure 1 could be instantiated with the following process:

1. Light nodes start a request to run services.
2. Full nodes ask to double check service requirements on data oracles.
3. National repositories provide data feed to oracles and confirm service requirements through national market API frameworks.
4. Full nodes allow the terms of service.
5. Light nodes propose to update the ledger for validation.
6. Light nodes execute the services and transfer information to full nodes.
7. The ledger is updated on the DAO's full node validators and propagated to light nodes cross-border.

IV. Policy Recommendations

Completely decentralized finance is currently not in scope with respect to MiCA, leaving the question of how best to regulate DeFi still an open one. Taking into account the FISMA paper and building on the conceptual framework explained above, the following policy recommendations have been identified as crucial next steps which would be implemented to ensure consumer protection and innovation continue to develop in parallel at EU level:

1. DAO legal recognition within Future European Regulations or Directives

With a corresponding legal entity status for DAOs as governance structures, they could outsource off-chain reference data to public oracles. This information could be stored in tokens and in an Ethereum environment (for example) such information could then be locked to validators.

User >> oracle >> information >> validators >> DAOs >> validators update block

The legal nature of DAOs – apart from several legislative attempts to create a legal framework for a limited liability environment for such entities – has been discussed at length. To date, they do not fit the conventional legal possibilities and assessment criteria. While it might be feasible to deem them part of the already existing legal entity framework, thus forcing them into corporate forms that will not fit the intended purpose, such a decision would most certainly diminish their potential. It is therefore believed that DAOs need a legally certain and firm recognition at European law.

2. National API repositories integrated into EU oracle frameworks supported by legal recognitions (MiCA) and open-source arrangements (EBSI) to specific market-oriented use cases

A public, open source, and standardized API data framework could be the key to developing and harmonizing the oracles market and offerings for specific services (e.g. credit rating or identifications). It would be beneficial to also include data references at the European project level (e.g. European Blockchain Service Infrastructure, EBSI). This would allow the administrations of different member states to develop interoperable off chain solutions and provide more quality data on chain. Data should be verifiable in the real economy: public, hard, cheap to obtain and static

3. SoulBound token recognition within MiCA, eIDAS

SoulBound Tokens are non-transferable tokens representing a person's identity on the network. This could include work history, medical records, and any information that develops an entity or a person. The accounts that issue or hold this type of record are known as 'Souls.' In the scope of DeFi services we have found SoulBound tokens can play a key role also as complements to other identification standards (e.g. W3C Credentials) work in other service areas (e.g. Public Administrations).

Integrating concepts of SBTs would allow for an agnostic treatment of identification frameworks and compatibility for the reference architecture with Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) for individual users. Hard information (LEI codes or UID) could also be verified under this framework for KYB purposes. Furthermore, soulbound tokens much like other forms of verification technologies would qualify the owners of SBTs as data controllers under GDPR. Another piece of legislation, where additional guidance can be found is the Draft Data Act possibly as a form of personal information management systems (PIMS).

4. A voluntary compliance/supervision mechanism over off/on chain data flows provided through a modular approach and addressing or reducing public/market specific risks to promote risk management practices.

Voluntary compliance potentially represents a smart tool for enlarging the enforcing market policies of DeFi services on the condition that incentives find balance between market attractiveness and compliance need. Soulbound tokens with B2B standards like LEI requirements can represent a solution to set a legal identification framework for DeFi service providers. The DeFi universe also includes entities that are not or cannot be recognized under the standard legal identity system. In particular, DeFi protocols do not bear means of enforcement from standard policy frameworks. Hence, we consider an open policy framework with attractive benefits to DeFi services that can produce voluntary compliance. In such a setting, entities and protocols voluntarily seek to comply with a given set of policy requirements - as opposed to exclusively formal qualifications, formats, and supervisory thresholds - in order to obtain a public stamp of approval and other potential benefits. On the part of DeFi, public compliance produces public signals of quality and good intentions.

On the part of policy institutions, attracting DeFi activity under this framework extends enforceability of rules and guidance. A voluntary mechanism is feasible because its implementation is compatible with the information structure of DeFi services: private information can be linked to public activity, while the other way around is not. Technologically, this result could be obtained through the public licensing of supervisor-approved, non-tradable and non-fungible tokens (e.g., public ID NFT). These tokens would be associated with one or multiple public addresses and serve as legally recognized proof of compliance in the DeFi ecosystem. However it would also require new rules specific to DeFi services and a carefully designed set of incentives and supervisory powers to make compliance attractable enough

Supervision is in theory intrinsically against DeFi services but both could and should be accepted by the market to address or reduce public or market specific risks and promote risk management practices. In order to be effective it should support on chain data analysis tools such as an off chain oracle data feed. In addition to that, any supervisory entity would be offered a safe and effective way to gain access to DeFi activity to carry out its mandate to provide for functioning capital markets while ensuring a maximum level of consumer protection paired with creating an environment where innovative ideas and entities are enabled to develop. Such a rationale could be found in an approach focusing on the specific underlying business services and products operated by DeFi. For example, those which do not see stringent restrictions by public interests may opt for voluntary disclosure. In other cases a slight supervision mode may be required to support capital and consumer protection which could be balanced by public observatories.

5. Further ensuring compliance through public observatories

Given the inherently different structure of DeFi projects, we identify a role for a public observatory of DeFi activity operated by a public authority. Such an institution would deploy public investigations and issue opinions and warnings publicly about specific DeFi protocols, practices and public address activities. Furthermore, when applying our information view of DeFi, we observe that, while auditing of on-chain protocols may be complete and consistent, auditing off-chain protocols might require auditing auxiliaries outside the public reach - in particular oracles, potentially linking back to traditional legal system structures. While this proposal does not entail enforcement power it however covers the entire universe of public protocols.

Traditional financial supervision includes the monitoring of financial institutions' activity. Such a task is achieved by processing both public and (more importantly) private and sensitive information in order to ensure excessive risk and illegal activities are under control. Warnings, sanctions and other forms of interventions may ensue in case of malpractice. Monitoring processes and their outcomes are usually confidential - though extreme outcomes may become public matters. While it is part of the DeFi design to prevent external arbitrary powers to intervene, the transparency of both protocols and historical activity allows in theory for an adapted form of supervision.

6. Oracles as a nexus for both stability and supervisory requirements and opportunities

The reliability of oracle services also plays a role in determining adoption and stability. Trust in oracles includes at least two dimensions: trust in the production of information by the oracle and trust in the transmission of the information from the oracle to the contract. While the first one may be driven by economic incentives, the second one relates to risks such as operational failure or cyber-attacks.

Utilizing oracles for supervisory and policy purposes would result in information that is verifiable in the real economy, public and open to all interested parties, readily obtainable and reliable. In this view, public support for establishing standardized frameworks for specific data production, processes and APIs could promote competition, innovation, adoption and coordination among heterogeneous agents including consumers, protocol designers and oracles. Similar initiatives could be directed to the development of security standards and disclosure guidelines for ensuring conflicts of interest are avoided between oracles and other contracting parties. Compared to actual DeFi actors, several forms of oracles have a direct presence in the economy. As such, providing a legal framework for them to operate could substantally improve efficiency and trust. First, a legal framework would introduce liability to an oracles activity.

Licensed oracles could therefore produce reliable information on candidate customers which could then be used by DeFi protocol. For instance, Know-Your-Customer (KYC) non-fungible tokens could be produced by specialized oracles under a public policy framework. These non-tradable tokens would then be recognized and used by the customers to undertake financial activities in DeFi. Similarly, credit-scoring non-fungible tokens could be produced in order to expand the contracting space of lending protocols. Note that both cases can be achieved while keeping identities private on-chain. That is, ownership of a token would convey information about the user without necessarily revealing the identity of the user.