IN DECENTRALIZED FINANCE NOBODY KNOWS YOU ARE A DOG

Vincent Gramlich
FIM Research Center,
Frankfurt University of
Applied Sciences
vincent.gramlich@fim-rc.de

Tobias Guggenberger
FIM Research Center,
University of Bayreuth
tobias.guggenberger@fim-rc.de

Marc Principato
FIM Research Center,
University of Bayreuth
marc.principato@fim-rc.de

Benjamin Schellinger
Blockchain Research Lab
schellinger@
blockchainresearchlab.org

Sebastian Duda
FIM Research Center,
Fraunhofer FIT
sebastian.duda@fit.fraunhofer.de

Jens-Christian Stoetzer
FIM Research Center,
University of Bayreuth
jens.stoetzer@fim-rc.de

Abstract

Identities are an essential aspect of information systems (IS) as they allow users of a digital ecosystem to interact, build trust, and form relationships. Decentralized finance (DeFi) is a digital, blockchain-based ecosystem that has seen tremendous growth in the last years, however, it struggles with current identity implementations. While academics and practitioners have identified numerous implications, a scientific systematization of the role of identities in DeFi and their potentials and challenges is missing. By conducting a multivocal literature review, we rigorously gather the current knowledge and aggregate the different perspectives and concepts to present (I) a comprehensive conceptualization of identities in DeFi, (II) their potentials and challenges, and (III) concepts to manage the tension in between. Thereby, we aim to lay a foundation for future research on identities that increase DeFi's security, efficiency, and adoption while minimizing or eliminating the drawbacks for data privacy and censorship.

Keywords: Decentralized Finance, Blockchain, Anonymity, Identity, SSI

1 Introduction

Developments in crypto finance over the past few years have contributed to the emergence of a decentralized financial ecosystem, commonly referred to as Decentralized Finance (DeFi) (Schär, 2021). DeFi comprises various financial applications that enable trustless and decentralized financial activities (Gramlich et al., 2023). DeFi's popularity is, among others, emphasized by the total value of assets, which peaked at approx. 180 billion USD in December 2021 and is still beyond 60 billion USD (DeFi Llama, 2022). As DeFi contains significant funds and opportunities for business operations, a rich financial service sector has formed around DeFi services. Besides crypto-native businesses like centralized exchanges (CEXes), e.g., Binance, institutions from the existing financial system, such as traditional banks, e.g., JP Morgan, show increasing interest and involvement in this upcoming ecosystem too (Qin et al., 2021).

While DeFi boasts advantages, its widespread adoption remains limited. This is particularly attributed to the absence of real-world identity linkability, where users are identified solely by blockchain addresses and key pairs, undermining trust, security, and compliance (Voskobojnikov et al., 2021). The missing link of user identities hampers financial product functionality like undercollateralized loans and secure governance (Schär, 2021; Werner et al., 2021). Furthermore, it impedes KYC processes for AML and CFT compliance which hinders adoption from financial institution and enables illicit activities (Gramlich et al., 2023; Qin et al., 2021). Regulatory actions like OFAC's ban of Tornado Cash, a protocol that enables untraceable money transfers, further highlight associated risks (U.S. Department of the Treasury, 2022).

Even though the importance of identities is commonly emphasized in the literature on DeFi, questions about the potentials and challenges of current identity systems remain mainly unexplored (Gramlich et al., 2023). Some proposed approaches to balance the trade-off between privacy preservation and transparency, e.g., Jabotinsky and Lavi (2021), aim at centralizing identities within a decentralized ecosystem, thus creating further areas of tension. Hence, we follow the suggestion of Alvesson and Sandberg (2011) to problematize these existing approaches to identities in DeFi.

Aiming to lay a foundation for further research, we seek to answer the following research questions:

URI: https://hdl.handle.net/10125/106932
978-0-9981331-7-1

RQ1: How can identities in DeFi be conceptualized and what are their potentials and challenges?
RQ2: How to manage the tension between potentials and challenges of identities in DeFi?

To answer our research questions, we first aimed to identify the most relevant literature using a multivocal literature review. We then aggregated and systematically analyzed the different perspectives and concepts to form a conceptualization of identities in DeFi. In the next step, we identified potentials and challenges regarding identities in DeFi. Finally, we brought together concepts to manage the tension in between the potentials and challenges. After presenting these results, we conclude with a summary and an outlook for future research.

2 Foundations

2.1 Identity Concepts in Information Systems Research

Identities in IS research play a crucial role in identification, authentication, and authorization (Allen, 2016). They facilitate relationships and trust, representing a fundamental concept in people's lives (Strüker et al., 2021). Within IS literature, identity and access management (IAM) paradigms fall along a continuum between centralized and decentralized, with varying levels of entities' control over their identities (Tobin & Reed, 2016). The Self-Sovereign Identity (SSI) paradigm aims to maximize the users control over their identity and is thus considered the most decentralized, although a universally accepted definition for SSI is lacking (Guggenberger, Kühne, et al., 2023; Strüker et al., 2021).

The concept of identity involves the interplay between an entity and its attributes. An entity represents a collection of attributes, while an identity encompasses a subset of these attributes (Camp, 2004; Clauß & Köhntopp, 2001). Identifiers are specific attributes that uniquely establish the identity of an entity within a specific identity space. For instance, in the healthcare system, social security numbers (SSNs) serve as identifiers to uniquely identify patients (Allen, 2016; Camp, 2004). These identifiers connect entities to their other attributes. Entities can assert their identity by providing these identifiers, such as Alice providing her SSN for a doctor's appointment (Clauß & Köhntopp, 2001). However, verifying the claimed identity requires authentication through credentials like a social security card (Camp, 2004). Once an entity's identity is authenticated, resources can be authorized based on the attributes associated with the identity (Camp, 2004). For example, Alice's healthcare identity, would be checked to confirm her appointment registration and allow her to see a doctor.

2.2 Decentralized Finance

Decentralized finance (DeFi) is a rich and disintermediated financial ecosystem based on smart contracts and public blockchains (Schär, 2021). DeFi's goal is to create an efficient, permissionless, and open financial system in which anyone can use and create financial services and instruments (Chen & Bellavitis, 2020; Gramlich et al., 2023).

Bitcoin emerged from the financial crisis of 2008 as the first manifestation of a blockchain, and its origin can be attributed to distrust in authorities (Nakamoto, 2008). While Bitcoin introduced the concept of a trustless and decentralized payment system, its functionality is limited to the transfer of its native cryptocurrency bitcoin (Gramlich et al., 2022). The introduction of the Ethereum blockchain incorporated programmability through protocols, referred to as "smart contracts" (Buterin, 2014). Smart contracts are highly interoperable and are used for building various decentralized applications (Dapps) (Schär, 2021). In addition, they enable non-native cryptocurrencies (tokens) that can express a variety of assets in the form of fungible tokens and non-fungible tokens (NFTs) (Sunyaev et al., 2021). Owing to these technical innovations, a rich and disintermediated financial ecosystem based on smart contracts on top of the public infrastructural blockchain layer has formed, i.e., decentralized finance (Schär, 2021; Werner et al., 2021). DeFi's goal is to create an efficient, permissionless, and open financial system in which anyone can use and create financial services and instruments (Chen & Bellavitis, 2020).

To interact with the blockchain systems in DeFi, an externally-owned account (EOA) is created by randomly picking a private key and cryptographically deriving its associated public key, which is then translated into a blockchain address, serving as the unique identifier for the on-chain identity (Butijn et al., 2020; Jensen et al., 2021). In this context, on-chain denotes all the information that is visible on the blockchain, e.g., blockchain addresses or their transactions, while every other information is denoted as off-chain. Since the blockchain stores associated information regarding this identifier, ensuring the security of the private key (the credential to this identity) is of utmost importance (Wang et al., 2021). In essence, the identification is made via blockchain addresses, the authentication is done via a private key acting as a credential, and the authorization is done via the attributes the identity (i.e., the account) offers

(Gramlich et al., 2022). For example, if the balance is above zero, then the transaction is authorized.

3 Method

In order to conceptualize identities and capture their potential and challenges in the field of DeFi, it is necessary to collect the relevant literature in these fields and synthesize its knowledge about existing constructs, as suggested by Compeau et al. (2022). Therefore, we employed a multivocal literature review (MLR) approach. Unlike traditional systematic literature reviews (SLRs) that focus solely on academic literature (AL), MLRs incorporate grey literature (GL) sources such as practitioner insights (Garousi et al., 2019). This ensures a more holistic analysis of the topic, particularly in technical areas of inquiry (Kamei et al., 2021). Further benefits include preventing publication bias (Kitchenham & Charters, 2007) and covering novel, practitioner-driven research fields (Gramlich et al., 2023). Given that DeFi is a community-led phenomenon and the exploration of identities within this context is a novel area of investigation, we contend that utilizing an MLR approach is ideally suited for our research undertaking.

Our MLR process followed the guidelines proposed by Garousi et al. (2019), which extend the well-established SLR process of Kitchenham and Charters (2007) to include GL. We developed a search string by collecting relevant and related terms via searches in GoogleScholar and Elicit.org for the terms "Decentralized Finance" and "Identity", respectively. By collecting terms, we were able to construct search strings, which were then iteratively sample-tested regarding the quality of hits in databases and the inclusion rate of items. "DeFi" and "DLT", for example, did not yield satisfying results. For our final search, we used the following search string:

("Decentralized Finance" OR "Decentralised Finance") AND ("Identity" OR "Identities" OR "SSI" OR "Identifier" OR "Identification" OR "ID")

We performed our final search at the end of April 2023 across the following databases: ACM Digital Library, AIS eLibrary, EBSCO Host, Emerald Insight, IEEE Xplore, Science Direct, Springer Link, Web of Science, and Wiley Online Library. This initial search yielded 339 literature items. To refine the sample, we defined inclusion and exclusion criteria applied in the title, abstract, and full-text filters (Kitchenham & Charters, 2007). Items that (I_1) explored the concept of identities in DeFi, (I_2) were published in peer-reviewed journals or conferences, (I_3) and had accessible full-texts included. We excluded items that (E_1) did not contribute to the state of knowledge (i.e., only mention the topic briefly) or (E_2) were not written in English. Through backward and forward searches, we expanded our sample with additional relevant literature. Ultimately, our final set comprised 19 items from academic sources. In parallel, we applied the same search string to four established GL databases: arXiv, Cryptology ePrint Archive, Google Scholar, and RePEc. This search yielded an initial set of 2609 GL items. To manage this extensive set, we employed the stopping criterion approach of Butijn et al. (2020), including items until we reached a page with more non-relevant than relevant items. Without duplicates, we obtained a GL set of 151 items and applied the same inclusion and exclusion criteria as for academic literature, resulting in 27 GL items. As GL items are typically not peer-reviewed and may vary in quality, we assessed them against the quality criteria proposed by Garousi et al. (2019). Items failing to meet at least ten criteria were excluded, leaving us with a final set of 23 GL items. In total, our MLR process yielded 42 items (19 AL + 23 GL) for analysis.

For data analysis, we follow the method for qualitative literature reviews as outlined in the method guidelines of Kitchenham and Charters (2007) and Garousi et al. (2019). We start with multiple researchers redundantly reading through the identified literature and filling out data extraction forms (Garousi et al., 2019; Kitchenham & Charters, 2007). After the data extraction, we synthesize the findings of the individual perspectives accordingly via coding into a coherent summarization, following the "Line of argument synthesis" of Kitchenham and Charters (Garousi et al., 2019). Finally, we report our results.

4 The Current State of Identities in Decentralized Finance

Our literature review has collected a broad range of publications. The following will present an aggregation of the most important results and is structured following our research questions. First, we present the aggregated concept of identities in DeFi. Afterward, we lay out the potentials of identities in DeFi by showcasing how the current lack of identities impairs the security, efficiency, and adoption of DeFi. Finally, we derive challenges of establishing identities in DeFi from the literature and outline techniques that interfere with current identification and de-anonymization in DeFi.

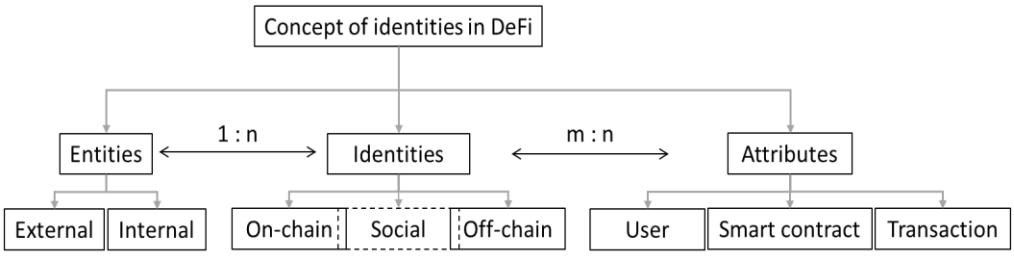

Figure 1. Concept of identities in DeFi.

4.1 Conceptualization of Identities in Decentralized Finance

To understand the concept of identities in DeFi it is important to distinguish between three main constructs, which are interrelated to the term identities. Figure 1 displays these three constructs: entities, identities, and attributes, as well as their different variations and their respective relationships. Every entity possesses attributes, while different identities of an entity can be expressed as different subsets of the set that contains all its attributes (Beres et al.).

In DeFi, entities can be differentiated into external and internal entities. Internal entities in DeFi exist organically within the system (i.e., on-chain), including transactions (Victor, 2020; Wright & Meier, 2021; Wu et al., 2021), smart contract-based entities such as tokens (Cernera et al., 2022; Das et al., 2022; Xia et al., 2021), and Dapps (Sun et al., 2022; Weyl et al., 2022). Internal entities in DeFi have only one identity that is stored on-chain and whose attributes are known to everyone in the system. For example, all the attributes of a transaction have to be known in order to process it and prevent double spending (Victor, 2020; Wu et al., 2021). The same applies to smart contract-based entities such as tokens and Dapps whose bytecode needs to be public so that the computations can be distributed and verified decentrally (Cernera et al., 2022; Das et al., 2022; Xia et al., 2021).

External entities in DeFi refer to every entity that exists off-chain such as CEXes (Jabotinsky & Lavi, 2021; Qin et al., 2021; Victor, 2020), tokenized artworks (Avrilionis & Hardjono, 2021; Barbereau et al., 2022; Das et al., 2022), or the user (Harwick & Caton, 2022; Linoy et al., 2019; Wang et al., 2021). They are represented by EOAs in the blockchain system (Chang et al., 2022; Wu et al., 2021) and are characterized by the transaction history and the blockchain address (Linoy et al., 2019; Wright & Meier, 2021; Wu et al., 2021). Transactions play an essential role in DeFi as they represent the interplay between on-chain identities (Beres et al.; Weyl et al., 2022; Wu et al., 2021). Important transaction attributes are the unique Tx ID (i.e., transaction hash) as well as the sender and receiver address (Linoy et al., 2019; Victor, 2020). As transactions have to be publicly verifiable to achieve consensus in DeFi, they enable the transaction history attribute of on-chain identities by linking transaction attributes to sender and receiver identifiers, which results in transparency benefits in DeFi (Victor, 2020; Wright & Meier, 2021; Wu et al., 2021).

External entities have off-chain identities, for example, the legal identity of users, i.e., the "real-world" identity, consisting of attributes that are personally identifiable information (PII) (Bansod & Ragha, 2022; Gao et al., 2021; Wu et al., 2021). Social identity refers to interaction between users and is two-sided. It can be on-chain, expressed through users transacting with each other (Kuśmierz & Overko, 2022; Pauwels et al., 2022; Weyl et al., 2022), and off-chain, expressed via social media or in-person interactions of DeFi users (e.g., in conventions) (Beres et al.; Wang et al., 2021; Weyl et al., 2022). The on-chain identity only contains on-chain attributes, is natively cost-free, and requires no linkage of other identities, such as the real-world identity or previous on-chain identities of a user for verification purposes or other measures to restrict access (Jensen et al., 2021; Wu et al., 2021). This circumstance is often subsumed under the permissionless, decentralization, and openness features of DeFi.

The identity concept, that we have outlined here, is based on a specific blockchain system, i.e., for other blockchain systems, on-chain identities are perceived off-chain and cannot be transferred seamlessly. Internal processing of off-chain data is not possible in this context, because it requires external integration with identities of other blockchain systems (Barbereau et al., 2022; Harwick & Caton, 2022; Zhao et al., 2022). This circumstance also explains the need for oracles in DeFi, which are, in essence, identity verifiers and curators between blockchains to bridge these hermetically separated data spaces and on-chain external entities by creating and managing trusted identities for them (Avrilionis & Hardjono, 2021; Barbereau et al., 2022; Zhao et al., 2022).

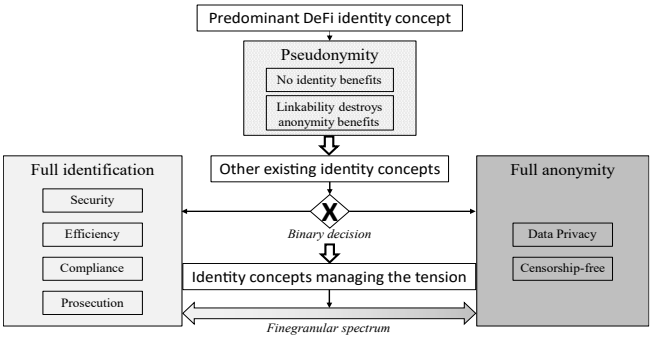

Figure 2. Tensions between identity concepts.

4.2 Potentials of identities in DeFi

DeFi is an inherently transparent system that uses the public viewability of on-chain identity attributes to execute and verify transactions (Gramlich et al., 2022; Liu et al., 2022; Qin et al., 2021). However, the publicly viewable on-chain identity is not directly linked to a real-world, i.e., external, identity. This results in the absence of a clear authority in such a system but also the non-existence of accountability structures (Jabotinsky & Lavi, 2021; Liu et al., 2022; Qin et al., 2021). That in turn, leads to significant drawbacks and hurdles for the current DeFi system that could be alleviated by a proper identity system, as displayed in Figure 2.

The lack of accountability comes with two main drawbacks that manifest in the design of DeFi application. The first is a security and complexity issue in DeFi's governance. As a replacement for accountability, incentive mechanisms are put in place to enforce the benevolent behavior of participants through game-theoretical approaches (Gramlich et al., 2022; Harwick & Caton, 2022; Liu et al., 2022). However, relying on incentives significantly limits DeFi's ability to become a secure and efficient financial system (Harwick & Caton, 2022; Kroon, 2021; Weyl et al., 2022). The security can be impaired by centralization in DeFi application governance, i.e., in the form of token ownership (Guggenberger, Schellinger, et al., 2023; Jensen et al., 2021; Kuśmierz & Overko, 2022; Sun et al., 2022) and the creation of an authority structure for the management of Dapps (Brennecke et al., 2022). Accumulating power in a system that is supposed to be decentralized and therefore does not ensure a clear accountability from the outset leads to security gaps in the system, e.g., attacks on parts of its governance (Gramlich et al., 2022; Jensen et al., 2021; Weyl et al., 2022).

The non-existence of identities also impairs DeFi's efficiency, for example, in the case of loans that need to be over-collateralized because a reputation score (e.g., a credit score) can easily be discarded by creating a new identity that is detached from the previous one (Gramlich et al., 2022; Guggenberger et al.; Harwick & Caton, 2022; Kroon, 2021). In general, on-chain governance mechanisms as a substitute for accountability structures limit DeFi's efficiency at the very moment when external information from off-chain is required (Avrilionis & Hardjono, 2021; Zhao et al., 2022). Furthermore, it severely limits DeFi's adoption of off-chain assets, such as the tokenization of physical artworks or assets in NFTs, as it is hard to ensure that the asset is an authentic on-chain representation of its off-chain version or whether it is a case of "asset identity theft" (Avrilionis & Hardjono, 2021; Barbereau et al., 2022; Das et al., 2022). Similarly, oracles suffer from non-persistent identities and require some degree of trust (Avrilionis & Hardjono, 2021; Harwick & Caton, 2022; Zhao et al., 2022).

Besides the DeFi inherent drawbacks of the non-existence of an identity system, it also presents hurdles and limitations in the form of regulatory compliance and adoption. Financial institutions in traditional financial systems are subject to specific regulations and laws to prevent illicit behavior, as they are responsible for the transfer and custody of assets and money (Jabotinsky & Lavi, 2021). Thus, compliance with financial regulation is a prerequisite for the market entry of these financial institutions and critical for the adoption of DeFi in general (Barbereau et al., 2022; Wright & Meier, 2021). Most noticeably, the effectiveness and enforcement of AML regulation are critical, in particular, for regulators (Jabotinsky & Lavi, 2021; Mell, 2019; Wright & Meier, 2021). Because of the absence of a persistent identity layer in DeFi, individual institutions that are subject to these regulations need to integrate KYC checks to ensure that the transaction parties are known to authorities, i.e., all institutions individually need to create a link between an on-chain and the real-world identity of an entity (Barbereau et al., 2022; Biryukov et al., 2018; Pauwels et al., 2022; Qin et al., 2021). However, following standard KYC processes to collect PII to link off-chain identity to on-chain identities for use in monitoring activities or accountability processes comes with several limitations. Firstly, it exposes the whole financial history of a user to all institutions that are required to collect this information, which introduces privacy issues (Hickey & Harrigan, 2022; Pauwels et al., 2022) and centralized points that represent a single point of failure and attract cyber-attacks (Das et al., 2022; Jabotinsky & Lavi, 2021). Secondly, the isolated and thus redundant implementation by all the individual institutions introduces inefficiency and hinders the scalability of a

large-spread adoption of DeFi (Gramlich et al., 2022; Qin et al., 2021). Moreover, it can often be bypassed by malicious actors, for example, by using multiple on-chain identities (Wright & Meier, 2021; Wu et al., 2021). Lastly, the question arises of how these could be technically implemented in smart contract-based entities since storing PII on-chain must be avoided to comply with data protection regulations, for example, with the EU's GDPR (Bansod & Ragha, 2022; Barbereau et al., 2022; Liu et al., 2022).

Besides the compliance issues, the separation of real-world and DeFi identities also enables illicit activities because it impedes the traceability of misbehaviors and the prosecution of malicious actors (Barbereau et al., 2022; Perdana et al., 2023). Thus, an identity system would come with a multitude of benefits, as displayed in Figure 2. In particular, re-introducing trust through a persistent identity for users and assets could facilitate reputation and would improve the security of DeFi and open up new design options for more efficient applications (Liu et al., 2022; Weyl et al., 2022; Zhao et al., 2022). Furthermore, comprehensive and verifiable identities in DeFi are a prerequisite for compliance with financial regulation, would help combat illicit activities, and could increase DeFi's adoption (Barbereau et al., 2022; Gramlich et al., 2023).

4.3 Challenges of identities in DeFi

Privacy is an important aspect of DeFi as the protection of sensitive financial data is important for compliance with data protection laws such as the EU's GDPR but also for user adoption in general (Bansod & Ragha, 2022; Barbereau et al., 2022; Liu et al., 2022). When it comes to data privacy, a critical differentiation must be made between pseudonymity and anonymity that denote different degrees of linkability between an entity and its identities, which also include its financial transactions. While anonymity refers to the complete absence of linkability, pseudonymity allows assigning specific identity aspects, e.g., DeFi transactions, to one pseudonym with no direct linkage to the entity behind it (Linoy et al., 2019; Qin et al., 2021; Wu et al., 2021).

As displayed in Figure 2, the predominant concept of DeFi is a pseudonymous system based on transparent and public blockchains that make transaction data accessible to everyone (Gramlich et al., 2022; Qin et al., 2021). With a combination of pseudonymity and transparency, however, additional external data can enable the association of the pseudonym to an entity and thus deanonymize all information associated with the pseudonym (Wu et al., 2021). As a result, a pseudonymous system with linkability loses the benefits of an anonymous system in the form of privacy and censorship resistance.

The simplest case of linkability is when users publicly share their blockchain address, i.e., on-chain identity, e.g., via social media (Chang et al., 2022; Wright & Meier, 2021). However, even without this direct way of deanonymization, it is possible to establish connections between pseudonyms and entities with forensic analyses that can be categorized into three different layers: network layer, application layer, and the transaction layer (Gao et al., 2021; Wang et al., 2021; Wu et al., 2021).

The analysis of the network layer is performed by connecting a full node to the peer-to-peer network of the blockchain, monitoring the transaction packages sent between other nodes, and inferring the original sender (Gao et al., 2021; Wang et al., 2021; Wu et al., 2021). When successful, one can link the IP address of a source node to its blockchain address, and thus, if the user itself runs the node potentially links his off-chain identity to his on-chain identity (Gao et al., 2021; Wang et al., 2021). The application layer analysis targets Dapps at the application front end (Wang et al., 2021). Backend analysis of Dapps is done by monitoring the code properties of smart contracts (Beres et al.; Linoy et al., 2019). It is also possible to extract information from end devices such as Web2 credentials (e.g., HTTP cookies), blockchain addresses, and transaction IDs to provide attribution (Chang et al., 2022; Winter et al., 2021). The most widely used analyses happen on the transaction layer, where the connection between different on-chain entities can be established by clustering addresses that show commonalities such as similar behavior or strong transactional connection (Gao et al., 2021; Hickey & Harrigan, 2022; Victor, 2020; Wu et al., 2021). All these methods allow for entity recognition (Beres et al.; Gao et al., 2021; Wang et al., 2021). When additional side-channel information (e.g., IP addresses or meta information) is available, full de-anonymization can be achieved (Gao et al., 2021; Hickey & Harrigan, 2022; Wu et al., 2021). This not only violates users' data privacy but also makes them vulnerable to censorship by providers of these different layers (Gramlich et al., 2022).

In conclusion, an identity system for DeFi needs to consider the benefits of an anonymous system and the various techniques that create linkability and de-anonymization to enable users to make intentional decisions regarding their identity usage and data privacy and protect them from censorship (Biryukov et al., 2018; Pauwels et al., 2022).

5 Managing the tension between potentials and challenges

As outlined above and displayed in Figure 2, DeFi is predominantly a pseudonymous ecosystem that has none of the benefits of a persistent identity but also misses the benefits of anonymity due to linkability. Most of the other existing identity concepts form a binary decision between full identification or full anonymity, with the respective benefits. However, the literature identifies a need for a more differentiated decision between these two poles and proposes concepts to manage the tension between the potentials and challenges of an identity system (Barbereau et al., 2022; Liu et al., 2022; Pauwels et al., 2022). Only a few proposals center around centralized identity management, such as using permissioned blockchains that link off-chain to on-chain identity by requiring PII at the infrastructure level before granting entry (Jabotinsky & Lavi, 2021; Mell, 2019) or using third parties that manage the IAM process and then post the result on-chain (Harwick & Caton, 2022). For public blockchain governance, more decentralized options could be feasible (Liu et al., 2022).

Most proposals for managing identity potentials while minimizing drawbacks focus on SSI-based approaches with identity proofs in the form of verifiable credentials (VCs) and presentations (VPs). In an SSI-based DeFi ecosystem, an identity issuer (a trusted third party for the application at hand) herby issues a cryptographic identity proof (i.e., a VC) to an entity that can use the VC to generate VPs to authenticate arbitrary claims that are made about attributes of the VC to a verifier, e.g., a smart contract of a DeFi service (Bansod & Ragha, 2022; Kroon, 2021; Weyl et al., 2022). As this paradigm allows for self-sovereign and seamless transfer of attributes between identities, it is commonly used to port attributes from a real-world identity over to the on-chain identity for usage in compliance processes such as KYC checks to prevent money laundering by encapsulating PII (Barbereau et al., 2022; Biryukov et al., 2018; Pauwels et al., 2022).

In addition, SSI can enable trust in an uncollateralized loan setting (Kroon, 2021) or the creation of verified digital identities for off-chain assets (Avrilionis & Hardjono, 2021), levering DeFi-based services. To comply with privacy requirements, ZKPs can be used for the VP so that only the minimal requested identity information is shared with the verifier, a feature commonly called "selective disclosure" (Barbereau et al., 2022; Kroon, 2021; Pauwels et al., 2022). Combined with the use of multiple identities, one can also enable a feature that we will call "selective privacy": VC holders can create identities that are used for purposes with differing degrees of identification and thus avoid that a verifier can link different proofed attributes to the same entity (Pauwels et al., 2022). The implementation of SSI in DeFi is commonly envisioned by IAM smart contracts that are used as a layer prior to accessing the financial functions of other smart contracts (Biryukov et al., 2018; Kroon, 2021; Pauwels et al., 2022). However, a significant limitation is that the standard SSI paradigm based on ZKPs is unilateral for two reasons: It fails to account for (I) a way to persistently share relevant attributes to every participant at once instead of only one verifier at a time and (II) "multi-party control" over the sharing of credentials that comprise attributes concerning more than one party (Weyl et al., 2022).

6 Conclusion and future research

To delve into the significance of identities within DeFi, it's crucial to first comprehend their definition in this context. Drawing from the identity paradigm prevalent in IS, we've adapted it to fit the DeFi landscape. While it encompasses the usual elements such as entities, identities, and attributes, their characteristics are notably distinct. The key variation is rooted in DeFi's reliance on a decentralized and untrusted framework, which prevents the generation of a consistent and universal identity for an entity based on a singular truth source.

Natively, DeFi doesn't mandate the linkage of an identity on one blockchain to the identities of its users on other blockchains. As a result, there isn't a singular DeFi identity, but rather separate on-chain identities for distinct DeFi blockchains. The absence of a consistent identity poses challenges for DeFi, particularly in security and efficiency. It also complicates regulatory compliance and efforts to counter illicit actions, thereby potentially slowing DeFi adoption. However, we see that there is a downside to integrating comprehensive identification, too, which introduces complexity and concerns about privacy and data protection regulations.

To address this inherent identity tradeoff, we analyze concepts that could be able to manage the tension between no and full identification. A potential solution provides the concept of SSI in combination with identity-representing tokens (e.g., ERC-725 or ERC-721). However, the challenge of designing various identity-representing tokens or SSI-based solution lie in their ability to support omnidirectional proofs and functionalities for multi-party-controlled credentials. Consequently, while the theoretical knowledge of SSI is available, the SSI paradigm's

practical use in DeFi still poses challenges that need to be tackled collaboratively by academia and practitioners. Therefore, we advocate for transdisciplinary research between academia and practice that includes DeFi experts, cryptographers, software engineers, regulators, and IAM researchers.

Despite our best efforts, this work has certain limitations. While our MLR method process ensured that we only included relevant literature, it is conceivable that we excluded some literature items with the formulation of our search string before the filter process started. As for our selection of GL, we limited the set to GL of the first tier and adopted a stopping criterion.

Nevertheless, we argue that our findings offer highly relevant and generalizable insights for the different stakeholders in DeFi. We envision that a consistent and secure identity system can improve DeFi's security, efficiency, regulatory and compliance, and ultimately, adoption. However, data privacy and the risk of censorship, two fundamental values of DeFi, also need to be considered. Thus, future research should focus on and extend concepts that manage the tension in between and allow for a more fine-granular and self-determined decision between identification and anonymity.

We conclude that, for achieving an efficient, secure, regulatory compliant, and widely adopted DeFi ecosystem, an identity concept is required that allows for privacy-preserving attribute sharing with multi-party control over attributes that concern multiple entities.

Acknowledgements

We gratefully acknowledge the Bavarian Ministry of Economic Affairs, Regional Development and Energy for their support of the project “Fraunhofer Blockchain Center (20-3066-2-6-14)” that made this paper possible.

References

Allen, C. (2016). *The Path to Self-Sovereign Identity*. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Alvesson, M., & Sandberg, J. (2011). Generating Research Questions Through Problematization. *Academy of Management Review*, *36*(2), 247–271. https://doi.org/10.5465/amr.2009.0188

Avrilionis, D., & Hardjono, T. (2021). Towards Blockchain-enabled Open Architectures for Scalable Digital Asset Platforms. *ArXiv*. https://doi.org/10.48550/arXiv.2110.12553

Bansod, S., & Ragha, L. (2022). Challenges in making blockchain privacy compliant for the digital world: Some measures. *Sādhanā*, *47*(3), 168. https://doi.org/10.1007/s12046-022-01931-1

Barbereau, T., Sedlmeir, J., Smethurst, R., Fridgen, G., & Rieger, A. (2022). Tokenization and Regulatory Compliance for Art and Collectibles Markets: From Regulators’ Demands for Transparency to Investors’ Demands for Privacy. In M. C. Lacity & H. Treiblmaier (Eds.), *Blockchains and the Token Economy* (pp. 213–236). Springer International Publishing. https://doi.org/10.1007/978-3-030-95108-5_8

Beres, F., Seres, I. A., Benczur, A. A., & Quintyne-Collins, M. Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users. In *2021 IEEE International Conference on Decentralized Applications and Infrastructures.* https://doi.org/10.1109/DAPPS52256.2021.00013

Biryukov, A., Khovratovich, D., & Tikhomirov, S. (2018). Privacy-preserving KYC on Ethereum. In *W. Prinz & P. Hoschka (Eds.),Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of theEuropean Society for Socially Embedded Technologies* (ISSN 2510-2591). https://doi.org/10.18420/blockchain201809

Brennecke, M., Guggenberger, T., Schellinger, B., & Urbach, N. (2022). The De-Central Bank in Decentralized Finance: A Case Study of MakerDAO. In *Proceedings of the 55th Hawaii International Conference on System Sciences*.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper*. https://ethereum.org/en/whitepaper/

Butijn, B.-J., Tamburri, D. A., & van Heuvel, W.-J. den (2020). Blockchains: a systematic multivocal literature review. *ACM Computing Surveys (CSUR)*, *53*(3), 1–37. https://doi.org/10.1145/3369052

Camp, L. J. (2004). Digital identity. *IEEE Technology and Society Magazine*, *23*(3), 34–41. https://doi.org/10.1109/MTAS.2004.1337889

Cernera, F., La Morgia, M., Mei, A., & Sassi, F. (2022). Token Spammers, Rug Pulls, and SniperBots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB). *ArXiv*. https://doi.org/10.48550/arXiv.2206.08202

Chang, E., Darcy, P., Choo, K.-K. R., & Le-Khac, N.-A. (2022). Forensic Artefact Discovery and Attribution from Android Cryptocurrency Wallet Applications. *ArXiv*. https://doi.org/10.48550/arXiv.2205.14611

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized

business models. *Journal of Business Venturing Insights*, *13*, e00151. https://doi.org/10.1016/j.jbvi.2019.e00151

Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks*, *37*(2), 205–219. https://doi.org/10.1016/S1389-1286(01)00217-1

Compeau, D., Correia, J., & Thatcher, J. (2022). When Constructs Become Obsolete: A Systematic Approach to Evaluating and Updating Constructs for Information Systems Research. *MIS Quarterly*, *46*(2), 679–712. https://doi.org/10.25300/MISQ/2022/15516

Das, D., Bose, P., Ruaro, N., Kruegel, C., & Vigna, G. (2022). Understanding Security Issues in the NFT Ecosystem. *ArXiv*. https://doi.org/10.48550/arXiv.2111.08893

DeFi Llama. (2022). *Total Value Locked (TVL) in DeFi*. https://defillama.com/#

Gao, Y., Shi, J., Wang, X., Shi, R., Yin, Z., & Yang, Y. (2021). Practical Deanonymization Attack in Ethereum Based on P2P Network Analysis. In (pp. 1402–1409). IEEE. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00191

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, *106*, 101–121. https://doi.org/10.1016/j.infsof.2018.09.006

Gramlich, V., Guggenberger, T., Principato, M., Schellinger, B., & Urbach, N. (2023). A multivocal literature review of decentralized finance: Current knowledge and future research avenues. *Electronic Markets*, *33*(1), 1–37. https://doi.org/10.1007/s12525-023-00637-4

Gramlich, V., Principato, M., Schellinger, B., Sedlmeir, J., Amend, J., Stramm, J., Zwede, T., Strüker, J., & Urbach, N. (2022). Decentralized Finance (DeFi): Foundations, Applications, Potentials, and Challenges. https://www.researchgate.net/publication/362058434_Decentralized_Finance_DeFi_Foundations_Applications_Potentials_and_Challenges

Guggenberger, T., Kuhn, M., & Schellinger, B. Insured? Good! Designing a Blockchain-based Credit Default Insurance System for DeFi Lending Protocols. In *MENACIS2021*. https://aisel.aisnet.org/menacis2021/8/

Guggenberger, T., Kühne, D., Schlatt, V., & Urbach, N. (2023). Designing a cross-organizational identity management system: Utilizing SSI for the certification of retailer attributes. *Electronic Markets*, *33*(1), 3. https://doi.org/10.1007/s12525-023-00620-z

Guggenberger, T., Schellinger, B., Wachter, V. von, & Urbach, N. (2023). Kickstarting blockchain: designing blockchain-based tokens for equity crowdfunding. *Electronic Commerce Research*, 1–35. https://doi.org/10.1007/s10660-022-09634-9

Harwick, C., & Caton, J. (2022). What's holding back blockchain finance? On the possibility of decentralized autonomous finance. *The Quarterly Review of Economics and Finance*, *84*, 420–429. https://doi.org/10.1016/j.qref.2020.09.006

Hickey, L., & Harrigan, M. (2022). The Bisq decentralised exchange: on the privacy cost of participation. *Blockchain: Research and Applications*, *3*(1), 100029. https://doi.org/10.1016/j.bcra.2021.100029

Jabotinsky, H. Y., & Lavi, M. (2021). Speak Out: Verifying and Unmasking Cryptocurrency User Identity. *Fordham Intell. Prop. Media & Ent. LJ*, *32*, 518. https://ir.lawnet.fordham.edu/iplj/vol32/iss3/1/

Jensen, J. R., Wachter, V. von, & Ross, O. (2021). How Decentralized is the Governance of Blockchain-based Finance: Empirical Evidence from four Governance Token Distributions. *ArXiv*. https://doi.org/10.48550/arXiv.2102.10096

Kamei, F., Pinto, G., Wiese, I., Ribeiro, M., & Soares, S. (2021). What Evidence We Would Miss If We Do Not Use Grey Literature? In F. Lanubile (Ed.) (pp. 1–11). ACM. https://doi.org/10.1145/3475716.3475777

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering, *EBSE-2007-01*. https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

Kroon, H. (2021). Introducing Self-Sovereign Identity and Identity as Collateral in Decentralized Finance. https://repository.tudelft.nl/islandora/object/uuid%3A5728bcf1-265a-49d0-b3f5-b6653c315b1d

Kuśmierz, B., & Overko, R. (2022). How centralized is decentralized? Comparison of wealth distribution in coins and tokens. *ArXiv*. https://doi.org/10.48550/arXiv.2207.01340

Linoy, S., Stakhanova, N., & Matyukhina, A. (2019). Exploring Ethereum's Blockchain Anonymity Using Smart Contract Code Attribution. In (pp. 1–9). IEEE. https://doi.org/10.23919/CNSM46954.2019.9012681

Liu, Y., Lu, Q., Yu, G., Paik, H.-Y., & Zhu, L. (2022). Defining blockchain governance principles: A comprehensive framework. *Information Systems*, *109*, 102090. https://doi.org/10.1016/j.is.2022.102090

Mell, P. (2019). Augmenting Fiat Currency with an Integrated Managed Cryptocurrency. *ICSEA 2019: The Fourteenth International Conference on Software Engineering Advances*, 83–90.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *White Paper*. https://bitcoin.org/bitcoin.pdf

Pauwels, P., Pirovich, J., Braunz, P., & Deeb, J. (2022). zkKYC in DeFi: An approach for implementing the zkKYC solution concept in Decentralized Finance. *Cryptology EPrint Archive*. https://eprint.iacr.org/2022/321

Perdana, A., HU, E. I., & Rianto (2023). Decentralized Finance (DeFi), Strengths Become Weaknesses: a Literature Survey. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(2), 397–404. https://doi.org/10.29207/resti.v7i2.4806

Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi -- Comparing Centralized to Decentralized Finance. *ArXiv*. https://doi.org/10.48550/arXiv.2106.08157

Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*, *103*(2). https://doi.org/10.20955/r.103.153-74

Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., & Völter, F. (2021). Self-Sovereign Identity - Foundations, Applications, and Potentials of Portable Digital Identities. *White Paper*. https://www.researchgate.net/publication/354653404_Self-Sovereign_Identity_-_Foundations_Applications_and_Potentials_of_Portable_Digital_Identities

Sun, X., Stasinakis, C., & Sermpinis, G. (2022). Decentralization illusion in DeFi: Evidence from MakerDAO. *ArXiv*. https://doi.org/10.48550/arXiv.2203.16612

Sunyaev, A., Kannengießer, N., Beck, R., Treiblmaier, H., Lacity, M., Kranz, J., Fridgen, G., Spankowski, U., & Luckow, A. (2021). Token Economy. *Business & Information Systems Engineering*, *63*(4), 457–478. https://doi.org/10.1007/s12599-021-00684-1

Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. *White Paper*. https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/

U.S. Department of the Treasury. (2022). *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*. https://home.treasury.gov/news/press-releases/jy0916

Victor, F. (2020). Address Clustering Heuristics for Ethereum. In J. Bonneau & N. Heninger (Eds.), *Financial Cryptography and Data Security* (Vol. 12059, pp. 617–633). Springer International Publishing. http://link.springer.com/10.1007/978-3-030-51280-4_33

Voskobojnikov, A., Abramova, S., Beznosov, K., & Böhme, R. (2021). Non-Adoption of Crypto-Assets: Exploring the Role of Trust, Self-Efficacy, and Risk. *ECIS 2021 Research Papers*. https://aisel.aisnet.org/ecis2021_rp/9

Wang, Y., Gou, G., Liu, C., Cui, M., Li, Z., & Xiong, G. (2021). Survey of security supervision on blockchain from the perspective of technology. *Journal of Information Security and Applications*, *60*. https://doi.org/10.1016/j.jisa.2021.102859

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). Sok: Decentralized finance (defi). *ArXiv*. https://doi.org/10.48550/arXiv.2101.08778

Weyl, E. G., Ohlhaver, P., & Buterin, V. (2022). Decentralized Society: Finding Web3's Soul. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4105763

Winter, P., Lorimer, A. H., Snyder, P., & Livshits, B. (2021). What's in Your Wallet? Privacy and Security Issues in Web 3.0. *ArXiv*. https://doi.org/10.48550/arXiv.2109.06836

Wright, A., & Meier, S. (2021). Analyzing FinCEN's Proposed Regulation Relating to AML and KYC Laws. In *Financial Cryptography and Data Security* (Vol. 12676, pp. 54–62). https://doi.org/10.1007/978-3-662-63958-0_5

Wu, J., Liu, J., Zhao, Y [Yijing], & Zheng, Z. (2021). Analysis of cryptocurrency transactions from a network perspective: An overview. *Journal of Network and Computer Applications*, *190*. https://doi.org/10.1016/j.jnca.2021.103139

Xia, P., Wang, H [Haoyu], Gao, B., Su, W., Yu, Z., Luo, X., Zhang, C., Xiao, X., & Xu, G. (2021). Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange. *Proc. ACM Meas. Anal. Comput. Syst.*, *5*(3). https://doi.org/10.1145/3491051

Zhao, Y [Yinjie], Kang, X., Li, T., Chu, C.-K., & Wang, H [Haiguang] (2022). Toward Trustworthy DeFi Oracles: Past, Present, and Future. *IEEE Access*, *10*, 60914–60928. https://doi.org/10.1109/ACCESS.2022.3179374