United Nations

ECE/CES/GE.20/2023/11

Economic and Social Council

Distr.: General
6 April 2023

English only

Economic Commission for Europe

Conference of European Statisticians

Group of Experts on National Accounts

Twenty-second session
Geneva, 25-27 April 2023
Item 4 of the provisional agenda
Digitalization

Potential Use of Decentralized Identities (DIDs) to Capture the Dynamic of Decentralized Finance (DeFi)

Prepared by Statistics Indonesia[1]

Summary

>   The exponential growth of the Decentralized Finance (DeFi) markets has raised concerns for statistical authorities because often they operate beyond the observation of formal authorities, which respectively could result in significant inaccuracy of economic statistics data. The peer-to-peer transactions inside these platforms, not facilitated by intermediaries make it difficult for authorities to engage in monitoring, identifying and recording the activities. As the main feature of the transactions is their anonymity, cooperating with DeFi platforms is also not a feasible option. The most practical solution is the use of blockchain analytics tools, which require a decentralized ID (DID).

> This paper is exploring the possibilities for statistical authorities to use DIDs to ensure correct identification and recording of decentralized financial activities.

[1] Prepared by Hadi Susanto.

I. Background information about Decentralized Finance and Decentralized Identities

1.   Digitalization has led to a significant increase in the volume of data involved and generated. It has also raised concerns regarding data security and privacy. Since the entirety of the modern financial system's operations is conducted digitally, financial data is the primary concern. Traditionally, this data has been managed and stored using centralized systems. A centralized system provides uncomplicated monitoring and management capabilities, such as putting everything on a desk. However, they come with their own risks and issues, such as a single point of failure and vulnerability to security threats.

2.   With Decentralized Finance (DeFi), blockchain-based decentralized systems offer an additional option. As depicted in Figure 1, DeFi could facilitate financial transactions without the need for intermediaries such as banks, allowing for greater access, transparency, and security. Decentralized Identities (DIDs), as a proposed protocol in DeFi, will enable individuals to have control over their personal data by permitting them to construct and manage their own identities, thereby decreasing reliance on centralized authorities. Together, DeFi and DIDs provide a decentralized alternative to traditional centralized systems, granting individuals greater control over their data and financial transactions.

Figure 1

Centralized vs Decentralized Financial Activities
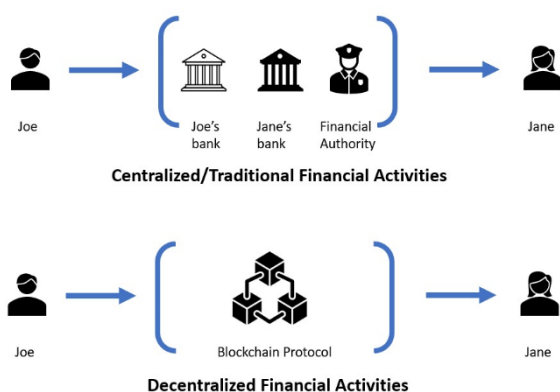
(source: https://bap-software.net/en/knowledge/defi-finance/)

3.   The World Wide Web Consortium (https://www.w3.org) is currently developing a standard for DIDs implementation. According to the World Wide Web Consortium, a DID is a new type of identifier that allows for verifiable and decentralized digital identities. A DID can be used to identify an individual, an organization, an object, or even an abstract entity. In contrast to traditional identifiers, DIDs are designed to be detached from centralized registries and any kind of identity provider.

II. Lack of Proper Identification in Statistical Data Collection in DeFi Ecosystem

4.   DeFi's escalating prevalence poses a significant challenge for official monitoring and statistics, particularly financial statistics. Since DeFi operates on a decentralized network and without intermediaries, it is exceedingly difficult for authorities to obtain accurate and trustworthy information regarding financial transactions and user profiles. As a characteristic of a decentralized environment, this lack of transparency and centralization would hinder the ability of authorities to monitor financial activities, detect fraud, and ensure compliance with laws and regulations.

5.   In addition, because DeFi is relatively new and rapidly evolving, there are instances of inadequate or inappropriate regulatory frameworks, which could exacerbate these difficulties. Therefore, policymakers and regulators must carefully consider the implications of DeFi and mitigate the risks by developing appropriate measures to resolve these challenges, while also allowing for the continued innovation and expansion of the field.

6.   The purpose of this paper is to investigate the potential for DIDs to facilitate statistical data collection in the DeFi ecosystem. This paper will primarily serve as a wake-up call for economic statisticians, given that DeFi is a new area of economic statistics and is still in the process of evolving into the most optimal form of the financial environment. Specifically, economic statisticians will be urged to develop a proper methodology to better capture DeFi as a statistical object.

III.   Overview of DeFi and Its Importance

7.   Managing DeFi will require appropriate regulatory frameworks to ensure compliance with the law and that it operates within legal boundaries. Due to the decentralized and complex nature of DeFi, regulatory authorities will need to carefully consider the most effective ways to foster innovation and growth while protecting against potential threats such as fraud, tax evasion, money laundering, and financial instability. Managing DeFi can be advantageous for the economy as a whole by fostering greater financial inclusion, efficiency, and stability through a proper equilibrium between **innovation** and **regulation**.

8.   Emphasis should be placed on the improvement of regulatory matters pertaining to DeFi activities, as this will inevitably increase transparency in DeFi ecosystems. This will result in improved access to transactions and participants for statistical observations.

IV.   Importance of Collecting Statistical Data in DeFi

9.   It is essential to acknowledge the increasing significance of DeFi platforms in the global financial system. DeFi platforms are gaining popularity as an alternative to traditional financial institutions, and their volume and variety of use are anticipated to increase in the coming years.

10.   Given the significance of the aforementioned DeFi platforms, national statistical agencies must covr transactions and participants in these new platforms. This is required to ensure that statistical data accurately reflect the entire scope of a country's financial activity.

11.   From the perspective of official statistics, collecting data on DeFi transactions and participants would be beneficial for the following reasons:

- It can enhance the veracity and completeness of financial statistics, ensuring that all financial activity is reflected in official statistics.

- It can provide valuable insight into the utilization and adoption of DeFi platforms in a country. This can aid policymakers and other stakeholders in their decision-making processes by identifying potential threats or opportunities within the DeFi ecosystem and financial system in general.

- Capturing data on DeFi transactions and participants can increase the ecosystem's transparency and accountability. This will help in building trust among users and investors and promote the sustainability of DeFi platform growth and development.

12.   The inclusion of DeFi transactions and participants in official statistical data is crucial for ensuring that financial statistics accurately reflect the full scope of financial activity in a country. It can provide valuable insights into the utilization and adoption of DeFi platforms and increase the ecosystem's transparency and accountability.

V.   Limitations of Traditional Identification Methods in DeFi

13.   Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures, although effective in current financial systems, will not work in DeFi due to the anonymous and decentralized nature of the network.

14.   The first limitation is the difficulty of verifying the true identity of a user, as it is common for users to conceal their identities by using pseudonyms or remaining anonymous. This makes it difficult for DeFi platforms to comply with KYC and AML regulations and consequently increases the likelihood of fraud, money laundering, and other illegal activities.

15.   Lastly, the lack of centralized authority in the DeFi space means that identification requirements and user activity monitoring are not enforced. This renders it incapable of ensuring regulatory compliance and holding users accountable for their actions.

16.   The limitations of traditional identification methods in the DeFi environment underscore the need for innovative and decentralized solutions that can effectively verify user identities, monitor transactions, and ensure regulatory compliance.

VI.   Introduction to DIDs and Their Potential to Resolve Identification Issues in DeFi

17.   DIDs are a form of decentralized identity that is gaining prominence in the DeFi ecosystem. DIDs are distinct identifiers anchored to a decentralized system, such as a blockchain, that can be used to authenticate and verify user identity without the need for centralized authorities.

18.   There are typically three types of DIDs in the DeFi environment, and they are as follows:

- Public DIDs are accessible to anyone and can be used for multiple purposes, such as authentication, authorization, and digital signatures.

- Private DIDs are only accessible to a limited group of people and are frequently used for more sensitive applications, such as access control and privacy protection.

- Hybrid DIDs, on the other hand, incorporate aspects of both public and private DIDs and are frequently used when both openness and privacy are necessary.

19.   DIDs utilize a decentralized identifier registry, which is typically maintained on a decentralized system such as a blockchain. When a user generates a DID, a unique identifier is generated and registered on the decentralized system. When the user interacts with DeFi platforms and protocols, this identifier can be used to authenticate and corroborate the user's identity.

20.   Figure 2 illustrates the process by which a user can create and use a DID in a DeFi application. The user first requests access to financial services from the DeFi application, which in turn requests the user to create a DID. The user then registers their DID with a DID registrar, which verifies their personal data. Once the user confirms their DID registration, the DeFi application can get the user's DID and personal information from the registrar. When the user requests to sign a financial transaction, they confirm the transaction with their DID. The DeFi application and DID registrar then verify the transaction with the user's DID, ensuring the transaction is legitimate and secure.

Figure 2

Mechanism of DIDs Workflow in DeFi
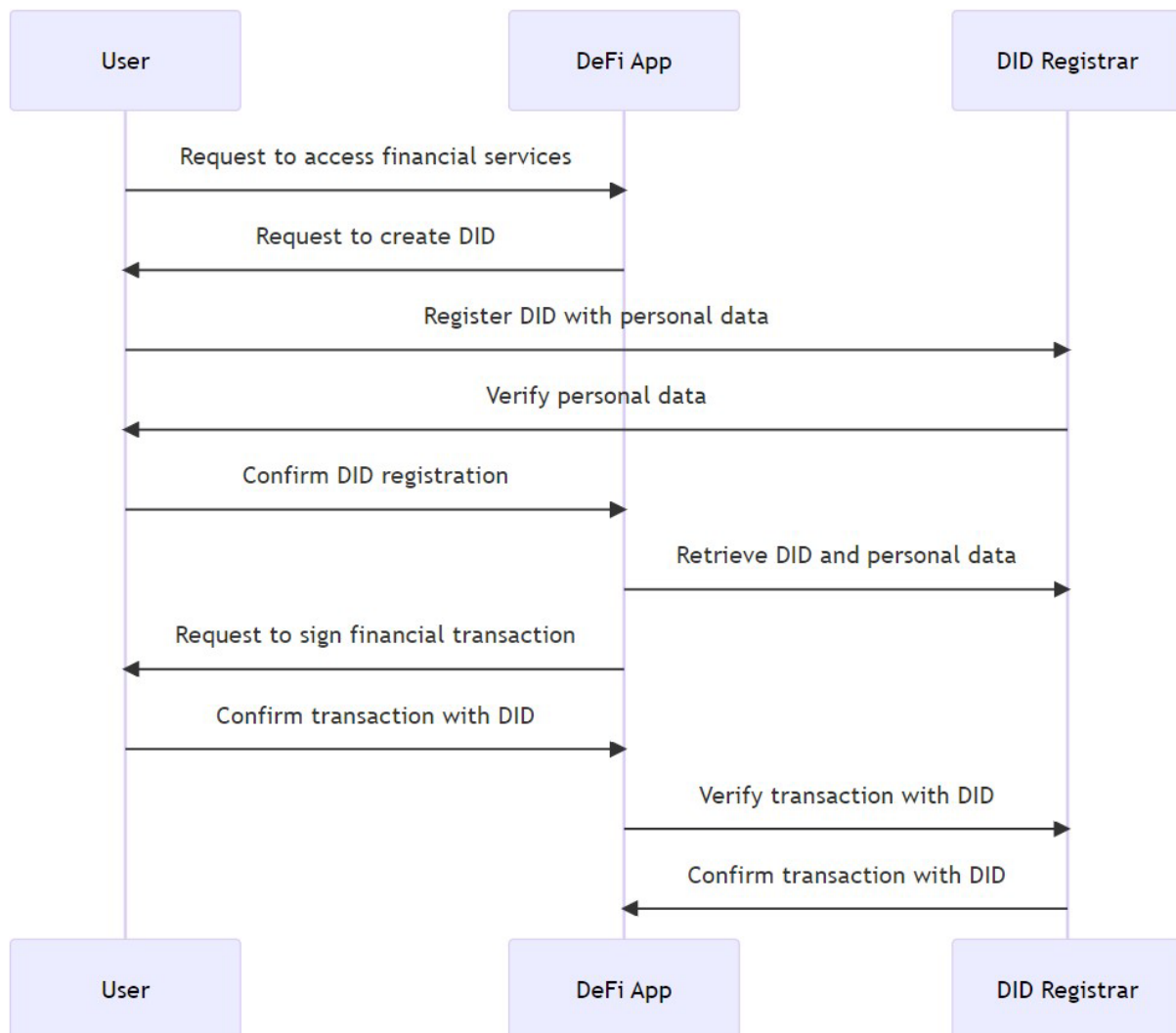
21.   One of the primary benefits of DIDs in DeFi is their decentralized nature, which eliminates the need for centralized authorities and decreases the risk of identity theft and other types of fraud. In addition, DIDs are designed to be interoperable, meaning that they can be used across various platforms and protocols, making them a valuable resource for DeFi users, developers, and authorities.

22.   DIDs have the potential to solve identification issues on DeFi transactions and participants. DIDs are intended to be a secure, decentralized, and interoperable identity solution compatible with multiple platforms and protocols.

23.   DIDs offer a more secure and trustworthy form of identity verification than traditional identification methods. DIDs generate unique, tamper-resistant identifiers that are anchored to a decentralized system, such as a blockchain, using public key cryptography. To pilfer or forge a user's identity, an attacker would need access to the user's private key.

24.   A further benefit of DIDs is that they can offer a more private method of identity verification than conventional methods. Because DIDs are decentralized and user-controlled, they enable individuals to maintain control over their personal information and determine when and how it is shared. This is especially crucial in the DeFi space, where users may be reluctant to share sensitive financial data with centralized authorities.

25.   DIDs can also aid in the resolution of the cross-platform data-sharing issue in DeFi. Because DIDs are interoperable, they can be utilized across various DeFi platforms and protocols, allowing users to maintain a consistent and dependable identity across applications. This can reduce the risk of inconsistent data and unreliable statistics and make it simpler for DeFi platforms to comply with regulatory requirements.

26.   According to the World Wide Web Consortium, there are 10 goals to be achieved by adopting DIDs. Those goals are decentralization, control, privacy, security, proof-based, discoverability, interoperability, portability, simplicity, and extensibility. Some of the goals are closely related to the improvement of statistical methods in covering DeFi as the new area of financial statistics.

27.   Overall, DIDs have significant potential for resolving identification issues among DeFi transactions and participants. DIDs can help improve the overall reliability, security, and transparency of the DeFi ecosystem by offering a more secure, privacy-preserving, and interoperable method of identity verification.

VII.   Prior Studies on the Potential of DIDs in DeFi

28.   Several research studies have investigated the capability of DIDs to identify transactions and parties in DeFi.

29.   Research on decentralized digital identity management was arranged by researchers from the University of Tartu and Tallinn University of Technology, which proposes a blockchain-based solution for DID-based decentralized identity management. The authors say that DIDs can be used to verify and authorize users in the DeFi ecosystem, making transactions more secure and clear.

30.   The World Economic Forum has been investigating the potential for DIDs and other decentralized identity solutions to enhance the efficacy and security of financial services, including DeFi. The forum proposes that DIDs can aid in reducing the risk of deception and enhancing the privacy of customers in financial transactions.

31.   Several blockchain and DeFi companies are also actively developing and implementing DID solutions for identity management in the DeFi ecosystem.

32.   Researchers and industry professionals have acknowledged the potential of DIDs to identify transactions and parties in DeFi, and there is ongoing research and development in this area.

VIII.   Summary of the Goals of Implementing DIDs in DeFi

33.   Adopting DIDs for capturing statistics in DeFi can offer numerous advantages, including enhanced data quality, transparency, and security. Using DIDs can increase the precision and completeness of DeFi transaction data. DIDs provide a more secure and tamper-resistant form of identity verification, thereby decreasing the likelihood that fraudulent or incomplete data will be recorded.

34.   Second, the utilization of DIDs can improve the visibility and traceability of DeFi transactions. DIDs provide a unique identifier for each participant in a transaction, allowing for more precise and granular reporting of DeFi activities.

35.   Thirdly, DIDs can enhance the security and confidentiality of DeFi data. DIDs enable users to retain control over their confidential data, thereby reducing the risk of data breaches or misappropriation.

36.   Lastly, the adoption of DIDs for statistics collection in DeFi can facilitate international cooperation and standardization in data collection and reporting. DIDs provide a standardized and interoperable form of identity verification, allowing for more accurate and consistent reporting of DeFi activities across jurisdictions.

37.   Adopting DIDs for capturing statistics in DeFi can provide several benefits to statistical agencies, including enhanced data integrity, transparency, and security.

Additionally, it can promote international cooperation and standardization in data collection and reporting, thereby augmenting the comparability and utility of DeFi statistics across jurisdictions.

IX. Recommendations for future research and implementation of DIDs in DeFi

38.   The implementation of DIDs in the DeFi ecosystem has the potential to substantially improve the ecosystem's efficiency, transparency, and security. To assure the successful adoption and incorporation of DIDs in DeFi, a number of research and implementation areas should be prioritized.

39.   First, standardized and interoperable DID protocols that can be used across various DeFi platforms and protocols are required. This will necessitate collaboration and coordination between **regulatory authorities**, **DeFi developers**, and **blockchain companies** to ensure that DIDs can be seamlessly integrated into the existing DeFi infrastructure.

40.   Second, research on the impact of DIDs on financial inclusion and access to DeFi services is required. DIDs have the potential to increase the security and transparency of financial transactions, but they may also present barriers to entry for those who lack access to the required technology or infrastructure.

41.   Thirdly, research on the privacy implications of DIDs in DeFi is required. DIDs can provide a more private form of identity verification, but there are concerns that they may also facilitate new forms of unnecessary surveillance and monitoring by governments and other organizations.

42.   Lastly, international cooperation and standardization are required for the collection and reporting of DeFi transaction data. This will necessitate collaboration between DeFi actors, regulatory bodies, and statistical agencies to acquire and report DeFi data in a consistent and standardized manner.

43.   Overall, the implementation of DIDs in DeFi has the potential to revolutionize the conduct and recording of financial transactions. To ensure that DIDs are incorporated in a manner that fosters financial inclusion, privacy, and international cooperation, however, additional research and collaboration are required.