www.fsca.co.za

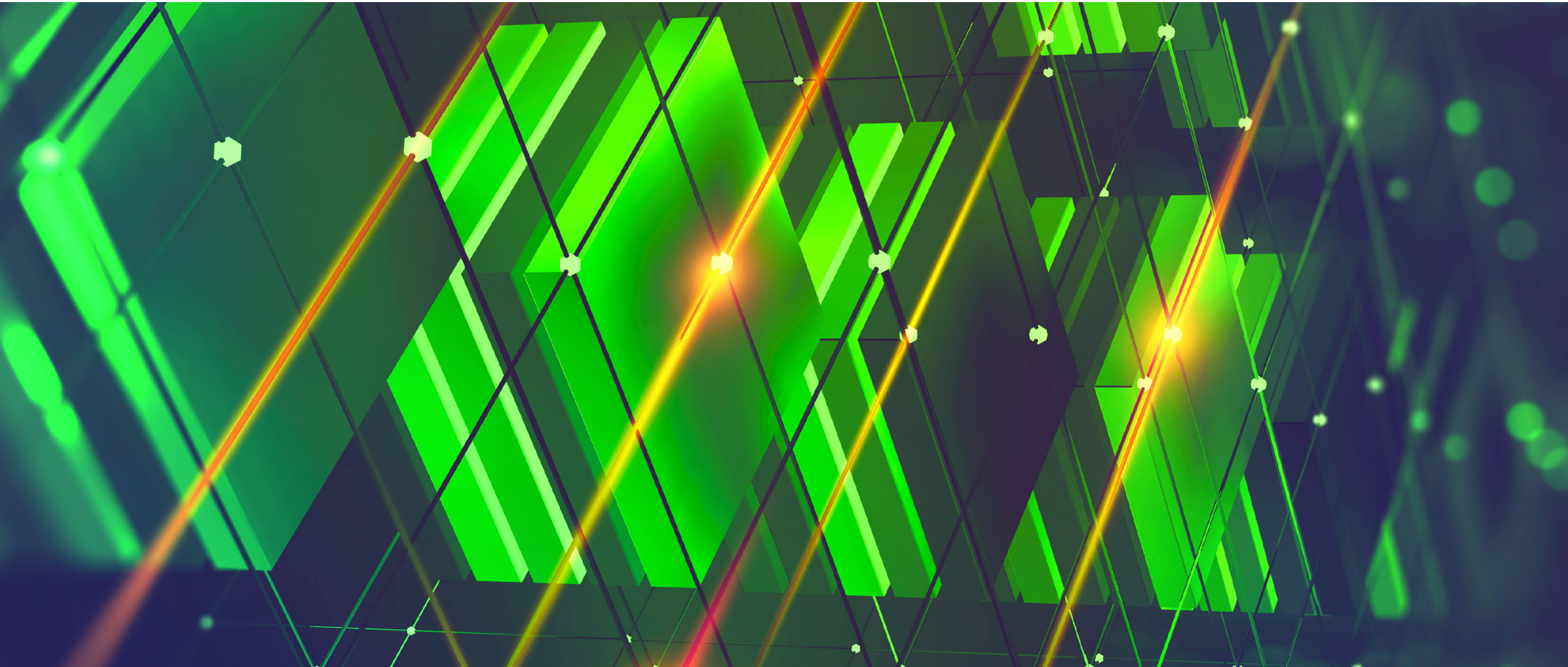
FSCA

Market Study: Decentralised Finance in South Africa

Authored by
Awelani Rahulani and
Nolwazi Hlophe

December 2024

DECENTRALISED FINANCE IN SOUTH AFRICA



CONTENTS

LIST OF TABLES

LIST OF FIGURES

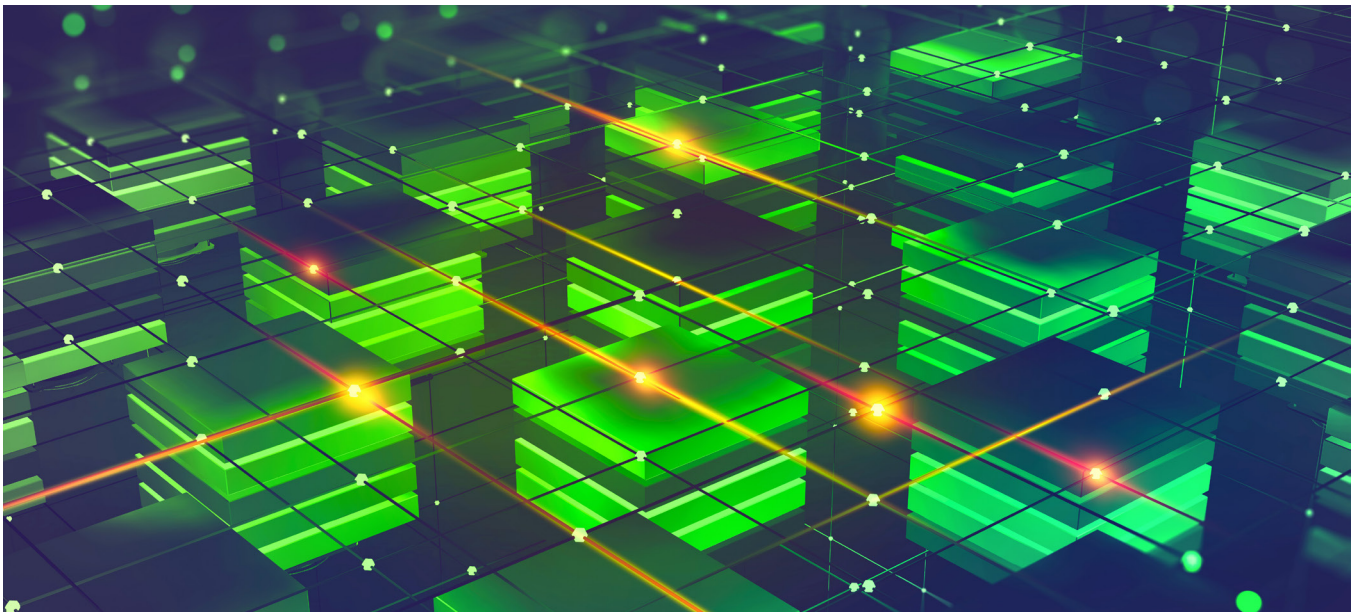
1. INTRODUCTION

The rapid evolution of financial technologies has ushered in a new era of decentralised finance (DeFi) transforming the traditional financial landscape. This research paper aims to explore the burgeoning DeFi ecosystem within the South African context. As DeFi platforms leverage blockchain technology to offer financial services without traditional intermediaries, they promise enhanced financial inclusion, transparency, and efficiency. But these claims remain to be tested.

The adoption of DeFi presents challenges in the form of security vulnerabilities and the potential for market volatility and manipulation, that present in unique ways relative to the traditional market. Financial education and increased investor awareness of how the market works, DeFi potential and its risks, will be critical. The extent of regulatory oversight will need to be carefully considered.

The purpose of this research report is to provide an overview of the DeFi landscape in South Africa, highlighting its potential benefits and associated risks. The study delves into the characteristics and various use cases of DeFi, such as payments, lending, borrowing, and asset management. It underscores the benefits DeFi can offer, including enhanced financial inclusion and increased transparency within the financial system. However, the report also addresses the inherent risks, associated with decentralisation and open systems, as effective DeFi relies on the integrity of smart contracts, the stability of its liquidity pools and the general sophistication and maturity of financial customers.

Market participants' views are explored, revealing a mix of optimism and caution regarding the future of DeFi. The report emphasises the critical importance of consumer protection and questions the true extent of decentralisation within the DeFi ecosystem, suggesting that elements of centralisation may persist.



2. BACKGROUND AND HISTORICAL CONTEXT

The year 2008 marked a watershed moment in the financial system. In the wake of the global economic crisis, Satoshi Nakamoto, a figure shrouded in anonymity, published the white paper titled Bitcoin: A Peer-to-Peer Electronic Cash System[1]. This document introduced Bitcoin, the first decentralised digital currency, and laid the foundation for blockchain technology.

At its core, blockchain is a distributed ledger – a digital record of transactions that is securely maintained and synchronised across a network of computers (nodes). This eliminates the need for a central authority to verify transactions, fostering transparency, immutability, and security within the system. The popularity of Bitcoin sparked a wave of innovation, paving the way for the emergence of DeFi.

Centralised finance (CeFi) and DeFi are two key components of the crypto finance ecosystem, each with its own unique characteristics[2].

CeFi refers to crypto asset and blockchain companies that operate like traditional financial systems, meaning a private central authority controls them as users are customers[3]. Examples of CeFi companies include Luno, VALR, Binance, and Coinbase[4]. These platforms offer a variety of services such as lending, borrowing, and margin trading[5] using crypto assets. However, funds are maintained outside of users' control and are exposed to threats if the exchange's security procedures fail.

DeFi platforms are blockchain based and are typically built using smart contracts, which are pieces of code that determine the rules a DeFi protocol operates under. Users who interact with DeFi smart contracts do what they would usually do in traditional finance (or centralised crypto finance) such as borrow money, make loans, or trade assets. The key difference is that all these activities take place without traditional intermediaries, and the entire operation runs on code[6].

The crypto asset financial system is mainly composed of CeFi and DeFi. It is important to obtain a view of the ecosystem between the traditional financial sector (TradFi), CeFi and DeFi as displayed in Table 1.

Table 1: Comparison between the TradFi, CeFi and DeFi ecosystem

CRYPTO FINANCIAL SYSTEM				
Function	**Service**	**Decentralised finance (DeFi)**	**Centralised Finance(CeFi)**	**Traditional finance**
Trading	Funds transfer	DeFi stablecoins (DAI)	CeFi stablecoins (USDT, USDC)	Traditional payment platforms
	Asset trading	Crypto asset DEX* (Uniswap)	Crypto CEX** (Binance, Coinbase)	Exchanges and OTC brokers
	Derivatives trading	Crypto derivatives DEX (Synthetix, dYdX)		
Lending	Secured lending	Crypto decentralised lending platforms (Aave, Compound)	Crypto centralised lending platforms (BlockFi, Celsius)	Broker-dealers active repo and securities lending
	Unsecured lending			Commercial banks and non-bank lenders
Investing	Investment vehicles	Crypto decentralised portfolios (Yearn, Convex)	Crypto funds (Grayscale, Galaxy)	Investment funds

*DEX: Decentralised exchange
**CEX: Centralised exchange

[1] Satoshi Nakamoto (2008), *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, available here.
[2] CoinDesk (2022), *"DeFi vs. CeFi in Crypto"*, available here.
[3] SoFi Learn (2023), *"CeFi vs DeFi: Similarities and Differences Compared"*, available here.
[4] CoinTelegraph (2024), *"DeFi vs. CeFi: Comparing decentralised to centralised finance"*, available here.
[5] CoinTelegraph (2024), *"DeFi vs. CeFi: Comparing decentralised to centralised finance"*, available here.
[6] CoinDesk (2022), *"DeFi vs. CeFi in Crypto"*, available here.

CeFi and DeFi are both used in the crypto environment, but they have different operational structures[7]. CeFi organisations operate similarly to traditional financial intermediaries, providing a familiar structure for users. This makes CeFi an easier and more familiar point of entry for people transitioning from traditional finance[8]. On the other hand, DeFi platforms can have a steep learning curve due to their decentralised nature and reliance on smart contracts[9]. Because DeFi platforms are built on new technologies and concepts, users often need to learn about blockchain, crypto asset wallets, private keys, and how to safely interact with smart contracts.

Although DeFi was initially envisioned to operate without intermediaries, financial intermediaries, including CeFi organisations, have been instrumental in the expansion of the crypto finance sector. For DeFi platforms to operate, user funds need to enter and exit the decentralised ecosystem, and most of its participants enter through centralised exchanges and intermediaries[10].

CeFi also provides a level of regulatory compliance that is often required by institutional investors and is seen as more secure due to its centralised nature[11]. The rise of CeFi is driven by its similarity to traditional finance, its role as a gateway to the crypto finance world, the crucial role of financial intermediaries, and its ability to provide regulatory compliance and security[12].

In November 2022, the collapse of FTX, a major CeFi exchange, further exposed vulnerabilities in the crypto ecosystem[13]. FTX's downfall was triggered by a liquidity crunch and allegations of mismanagement and fraud, revealing significant weaknesses in the governance and operational practices of multifunction crypto asset intermediaries[14]. The close relationship between FTX and its sister company, Alameda Research, exacerbated the situation as it became clear that customer funds were being misused to cover Alameda's trading losses[15]. This collapse not only shook investor confidence, but also highlighted the systemic risks posed by the lack of transparency and regulatory oversight in the crypto industry.

These incidents collectively demonstrated the fragility of both CeFi and DeFi systems, emphasising the need for robust risk management, greater transparency, and stronger regulatory frameworks to protect investors and ensure the stability of the crypto asset markets.

The early roots of DeFi can be traced back to the inception of Ethereum, a blockchain platform created by Vitalik Buterin and launched in 2015. Ethereum was designed to be a decentralised platform for building and running smart contracts[16]. These self-executing contracts, with the terms of the agreement directly written into code, allowed for the creation of decentralised applications (dApps) that could operate without intermediaries. dApps are developed by a diverse group of contributors, including blockchain developers, project teams, open source communities, independent developers, and established companies.

---

[7] CoinDesk (2022), *"DeFi vs. CeFi in Crypto"*, available here.
[8] CoinDesk (2022), *"DeFi vs. CeFi in Crypto"*, available here.
[9] CoinDesk (2022), *"DeFi vs. CeFi in Crypto"*, available here.
[10] Tech Crunch (2023), *"CeFi and DeFi in the face of regulation"*, available here.
[11] Techopedia (2024), *"DeFi vs. CeFi in 2024: Rivalry or Collaboration?"*, available here.
[12] CoinDesk (2022), *"DeFi vs. CeFi in Crypto"*, available here.
[13] CoinDesk (2022), *"8 Days in November: What Led to FTX's Sudden Collapse"*, available here.
[14] abc News (2024), *"A timeline of cryptocurrency exchange FTX's historic collapse"*, available here.
[15] NerdWallet (2024), *"FTX Crash: Timeline, Fallout and What Investors Should Know"*, available here.
[16] Smart contracts consist of code with the following characteristics: (i) A set of promises, (ii) Specified in digital form, (iii) Including protocols, (iv) Within which the parties perform on these promises.

The first significant DeFi project on Ethereum was MakerDAO, launched in 2017[17]. MakerDAO introduced the concept of a decentralised stablecoin, DAI, which is pegged to the US dollar and backed by collateral in the form of Ethereum[18]. This project demonstrated the potential of DeFi by providing a stable medium of exchange within the volatile crypto market[19]. Following MakerDAO, numerous other DeFi projects emerged, including Compound, Aave, and Uniswap, each offering unique financial protocols and contributing to the rapid growth of the DeFi ecosystem on Ethereum.

These early projects illustrated Ethereum's smart contract capabilities, paving the way for a new era of DeFi. DeFi applications, also known as DeFi protocols, are software programs built on blockchains, primarily the open-source Ethereum, which has the highest total value locked (TVL)[20] among all blockchains[21]. These protocols leverage blockchain technology to create an open, permissionless financial ecosystem that enables individuals to participate in financial activities traditionally facilitated by banks and other financial institutions.[22] Imagine a financial system where you can borrow, lend, trade or invest directly with other users, eliminating the need for intermediaries and potentially associated fees. This is the essence of DeFi. By interacting with DeFi protocols through user-friendly interfaces, consumers can engage in various financial activities, including lending and borrowing, trading, and derivatives, to name a few.

There is no universally accepted definition of DeFi. The Financial Stability Board (FSB) describes DeFi as "an umbrella term commonly used to describe a variety of services in crypto-asset markets that aim to replicate some functions of the traditional financial system (TradFi) while seemingly disintermediating their provision and decentralising their governance. The DeFi ecosystem has a multi-layered architecture that includes permissionless blockchains, self- executing code (or so-called smart contracts), DeFi protocols and purportedly decentralised applications (DApps)"[23]. Therefore, DeFi can be formally defined as a blockchain-based financial infrastructure that is open, trustless, permissionless, and highly interoperable, built on smart contract blockchain platforms like Ethereum, Tron, or Solana[24]. It is important to note that decentralised finance lacks a safety net.

The DeFi landscape is constantly woven with new protocols and applications emerging at an accelerated pace. Despite a strong start to June 2024, the TVL in DeFi protocols experienced an 8.7% decline[25]. This indicates some volatility in the market, possibly influenced by broader crypto market trends. These recent episodes of market turmoil have led to a discussion on whether and how the DeFi industry should be regulated.

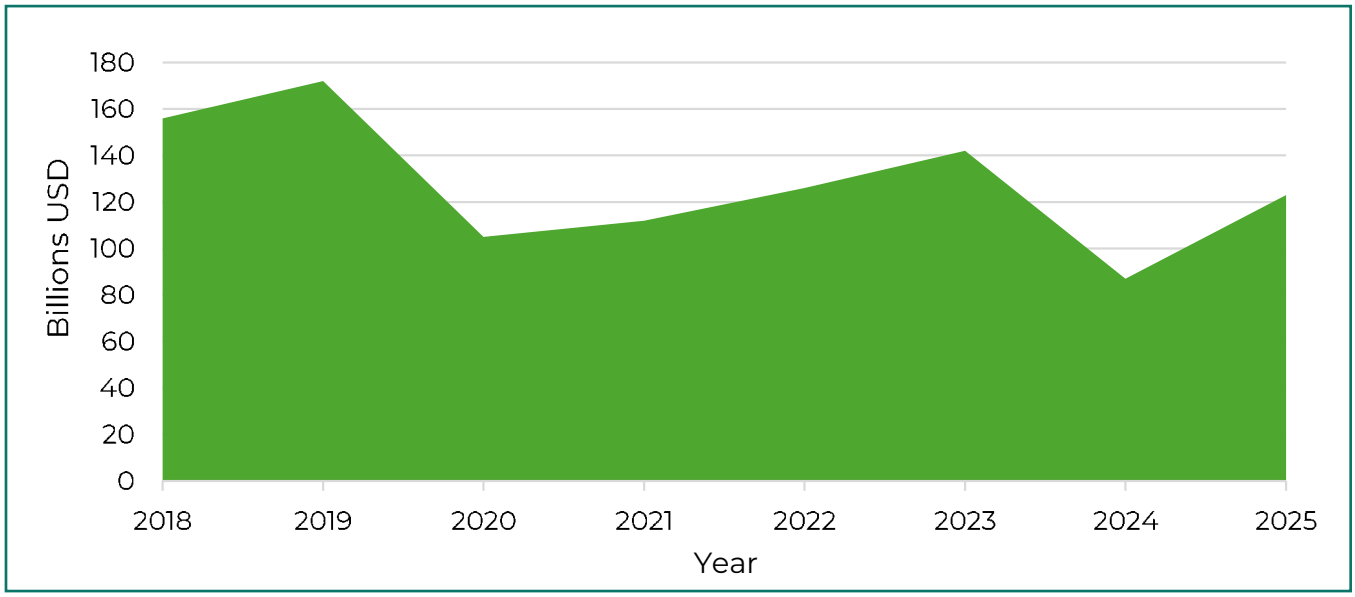
As of 31 January 2025, the TVL in DeFi protocols was UD$122.65 billion, where the total market capitalisation of stablecoins was US$217.3 billion[26] as seen in Figure 1.

South African crypto asset exchanges are increasingly introducing DeFi tokens on their platforms as they see a heightened appetite from the local market. In February 2024, Luno announced that they had added three new crypto assets to invest in that are leading in DeFi[27]. The DeFi market in South Africa is projected to reach revenue of approximately US$2.9 million in 2024. The number of DeFi users in South Africa is expected to reach 378 000 by 2025. User penetration is projected to remain at 0.62% in 2024 and 2025[28].

---

[17] MakerDAO (2019), *"BREAKING: Launch Date of Multi-Collateral Dai, the Dai Savings Rate, and More Announced at Devcon 5"*, available here.
[18] MakerDAO (2024), *"A better, smarter currency"*, available here.
[19] MakerDAO (2024), *"A better, smarter currency"*, available here.
[20] TVL is the total value locked. It is an Industry-reported measure of the total value of assets deposited in a DeFi protocol.
[21] CoinGecko (2024), *"Top Blockchains by Total Value Locked (TVL)"*, available here.
[22] Permissionless blockchain refers to a type of blockchain that allows anyone to join and participate in the network without needing any authorisation or approval. It is discussed more fully in the section of characteristics of decentralised finance.
[23] FSB (2023), *"The Financial Stability Risks of Decentralised Finance"*, available here.
[24] BIS (2023), *"The Technology of Decentralised Finance (DeFi)"*, available here.
[25] Crowdfund Insider (2024), *"Crypto Market Downturn Accompanied by DeFi Total Value Locked Experiencing 8.7% Decline in TVL in June – Report"*, available here.
[26] Defi Llama (2024), *"All Protocols"*, available here.
[27] IT Web (2024), *"SA crypto players diversify portfolios with DeFi coins"*, available here.
[28] Statista (2024), *"DeFi – South Africa"*, available here.

Figure 1: The global total value locked in DeFi



Source: DeFiLlama (2025)

Here's a glimpse into some of the largest and most influential DeFi protocols:

- **Uniswap:** Uniswap has experienced significant growth in its revenue. For example, in March 2024, Uniswap processed US$90.11 billion in monthly volume, which was a 97.1% increase from the previous period. This activity generated US$159.25 million in fees for market makers, reflecting a 73.3% increase[29]. This growth reflects the platform's expanding ecosystem and the increasing interest in decentralised exchanges (DEXs)[30].
- **Aave:** Aave is a DeFi lending and borrowing protocol that allows users to lend, borrow and earn interest in a variety of crypto assets. Aave was first deployed on the Ethereum network in January 2020. The Aave community treasury currently stands at US$132.5 million as of March 2024[31].
- **Curve Finance:** Curve Finance is a DEX specifically designed for efficient trading of stablecoins, which are crypto assets pegged to a stable asset like the US dollar. The significant drop in TVL on Curve Finance was due to a major exploit that occurred on July 30, 2023. This hack was caused by a vulnerability in the Vyper programming language, which is used to create some of Curve's liquidity pools. The specific issue was a malfunction in the re-entrancy guard, a mechanism designed to prevent multiple functions from being executed simultaneously[32]. Attackers exploited this vulnerability to withdraw funds from the pools without fully repaying them, resulting in a loss of over US$61 million[33]. Despite the hack, DeFi services revenue remains resilient, with recent weekly revenues around US$6.26 million[34].

These protocols, along with countless others, predominantly operate on Ethereum Virtual Machines (EVMs). EVMs are software platforms that mimic the functionality of the Ethereum blockchain, allowing developers to build and deploy DeFi applications on top of the Ethereum network. The interoperability offered by EVMs fosters innovation and scalability within the DeFi ecosystem.

---

[29] Uniswap Protocol Governance (2024), *"March '24 Uniswap Report"*, available here.
[30] A decentralised exchange (DEX) allows users to trade crypto assets directly with each other without an intermediary. DEXs use smart contracts on a blockchain to automate transactions. Users interact with the smart contracts to match buy and sell orders, often facilitated by liquidity pools where users deposit assets to earn fees. DEXs provide greater privacy and security since users maintain control of their funds. However, they can be more complex and may face liquidity challenges compared to centralised exchanges.
[31] CryptoMode (2024), *"What is Aave (AAVE)?"*, available here.
[32] CoinTelegraph (2023), *"Curve-Vyper exploit: The whole story so far"*, available here.
[33] CoinTelegraph (2023), *"Curve-Vyper exploit: The whole story so far"*, available here.
[34] Vardai, Z. (2023), *"DeFi revenue remains resilient despite Curve Finance hack"*, available here.

3. PROBLEM STATEMENT

DeFi activities are gaining traction in South Africa, presenting consumer protection challenges. While DeFi offers innovative financial solutions, its decentralised nature and elements of centralisation, such as centralised governance and reliance on centralised price oracles[35], pose unique risks. These include smart contract vulnerabilities, market manipulation, and the potential for significant financial losses due to fraud or platform failures.[36] The lack of robust regulatory oversight and clear consumer protection measures exacerbate these risks, leaving users vulnerable, and potentially undermining market trust.

Moreover, the key challenge for regulators in South Africa is that they may not have the jurisdiction to regulate DeFi protocols as these are spread all over the world and can be accessed by anyone with an internet connection. Therefore, it is imperative to understand these risks to be able to respond accordingly.

4. PURPOSE AND OBJECTIVES

The purpose of this market study is to better understand DeFi related activities currently being performed in South Africa; to highlight consumer exposure to these activities; and to identify risks that may negatively impact consumer well-being.

5. RESEARCH APPROACH

The study employed a “mixed-methods” approach. The FSCA obtained information related to DeFi-related activities in South Africa directly from crypto asset service providers (CASPs) by issuing a survey. The purpose of the survey was to a) assist the authority in obtaining a better understanding of DeFi-related activities that fintechs are currently performing and b) identify key use cases that we are seeing in South Africa, to better understand related consumer protection and market conduct risks.

Information submitted by the CASPs was augmented by interviews with experts in the field and desk-based research. The desk-based research drew information from different sources, including policy and academic texts, as well as national and international datasets from both public and private stakeholders.

[35] A price oracle provides real-time price data for assets to smart contracts on a blockchain. It gathers data from various sources, transmits it to the blockchain, and allows smart contracts to use this data for transactions and decisions. Reliable price oracles are essential for the stability and security of DeFi protocols.
[36] Smart contracts refer to self-executing contracts where the terms of the agreement are directly written into code. They automatically enforce and execute the terms when predefined conditions are met, typically on blockchain platforms like Ethereum.and are explained more fully in the section titled “Characteristics of decentralised finance”.

6. OVERVIEW OF THE DEFI ECOSYSTEM

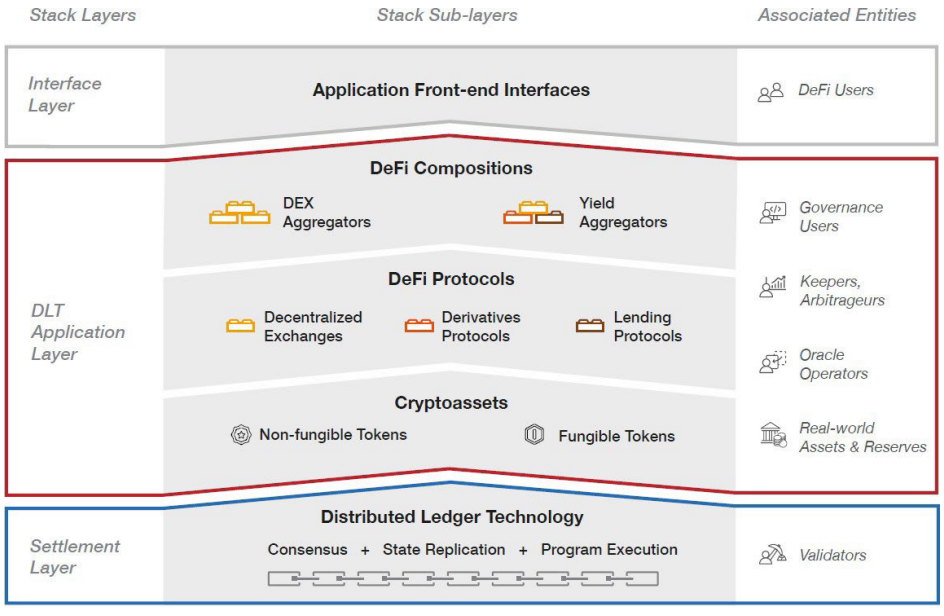
To understand the characteristics of DeFi and its solutions, it is important to comprehend how the system of DeFi works and the mechanics behind it.

6.1 CHARACTERISTICS OF DEFI

As previously described, blockchain technology is the foundational layer of the DeFi architecture and therefore underpins virtually all DeFi solutions. A blockchain is a form of distributed ledger technology (DLT) where all transactions are recorded and organised in blocks, which are linked together using cryptography. For the purposes of this paper, we will use blockchain to refer to a permissionless blockchain.

As illustrated in Figure 2, the DeFi ecosystem can be divided into three layers with five sub-layers, which are built on top of each other in a hierarchical manner, thereby creating the DeFi stack. Box 1 describes each layer in the DeFi technology stack.

Figure 2: The decentralised finance technology stack



Source: BIS (2023)

BOX 1: THE DECENTRALISED FINANCE STACK EXPLAINED

Interface Layer: Since distributed ledger technology (DLT) applications are built as smart contracts and are designed for developers to use with code, they don't have easy-to-use graphical tools for regular users. These interfaces help users input information into the DLT applications. DeFi applications use user-friendly interfaces like websites or mobile apps to help people interact with smart contracts, which are otherwise designed for developers and lack easy-to-use graphical tools. This front-end layer acts as a bridge, making it simpler for users to work with the underlying smart contracts.

Distributed Ledger Technology (DLT) Application Layer: The DLT application consists of applications which are implemented through smart contracts.

Crypto assets: The DLT applications help move value within the DeFi system. Crypto assets, like Tether (USDT), are created using special "token contracts." These contracts can either keep track of interchangeable tokens (fungible) or record who owns unique tokens (non-fungible) (BIS (2023)).

DeFi Protocols: This DLT application uses smart contracts and crypto assets to offer financial services. Different types of services include lending, derivatives, and DEXs. These services work through financial actions like pooling funds from many users, providing collateral, or swapping crypto assets. Some functions are unique to specific protocols, while others are common across different types of protocols.

DeFi Compositions: These are special DeFi protocols that use smart contracts to offer new financial services by leveraging other DeFi protocols. DEX aggregators help users find the best prices for swapping crypto assets by directing them to different DEXs. Yield aggregators, on the other hand, invest user funds in various DeFi protocols to maximise returns.

Settlement Layer: The settlement layer finalises financial transactions and settles obligations between parties. This is usually done using DLT like blockchains (e.g., Ethereum or Solana), which use consensus protocols to keep all computer nodes in sync. DLTs support smart contracts, which are essential for DeFi protocols. These platforms have their own native tokens or crypto assets, like ETH for Ethereum, that represent and transfer value in transactions or smart contract executions. These native tokens are part of the settlement layer, but are not created as smart contracts, unlike other tokens.

So, what are DeFi tokens? DeFi tokens are a variety of crypto assets that originate from automated, decentralised platforms and function through smart contracts. They offer users the ability to utilise a range of financial services that are constructed on the blockchain. DeFi tokens are built on, and often named for, their unique and native blockchain networks e.g., ETH is the native token for the Ethereum blockchain. Transactions of DeFi tokens are performed on-chain* (See Table 2 for the comparison of DeFi coins and currency).

Table 2: DeFi tokens in comparison with other forms of currency

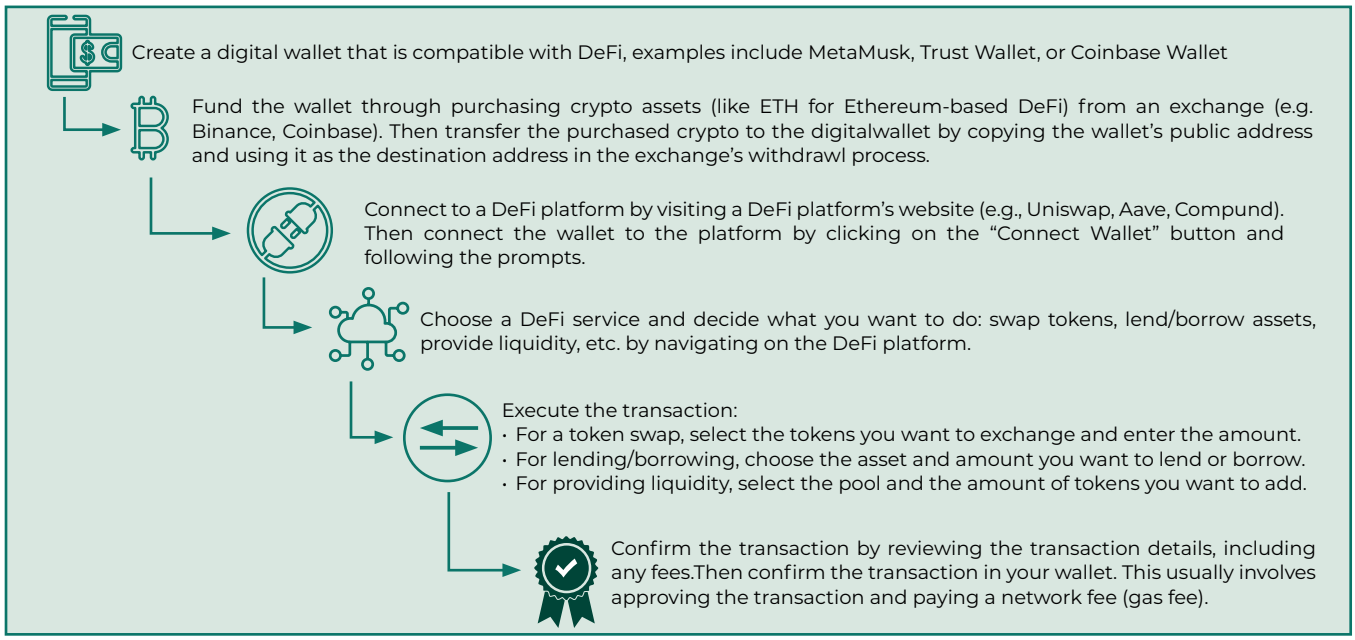
Key characteristics of money	Cash	Electronic Money	Crypto financial system	
			On-chain*	Off-chain**
Electronic	✗	✓	✓	✓
Sovereign legal tender	✓	✗	✗	✗
Self custody of funds	✓	✗	✓	✗
Financial regulated	✓	✓	✗	✓
Universaqlly accepted	✓	✗	✗	✗
Store of value	✓	✓	✗	✗
Unit of account	✓	✗	✗	✗
Instantaneous settlement	✓	✗	✓	✓

Source: Author's own

*DeFi records all the contractual and transaction details on the blockchain (i.e., on-chain).
**CeFi[37] relies on the private records of intermediaries, such as centralised exchanges and other platforms (i.e., off-chain)

How do you perform a transaction in the DeFi ecosystem? Figure 3 illustrates the process for performing a transaction in the DeFi ecosystem.

Figure 3: DeFi transaction process



The key concepts of DeFi are (i) blockchain technology, (ii) smart contracts, and (iii) tokenisation. These are broken down below according to their characteristics.

[37] CeFi is an abbreviation of centralised finance. Centralised finance describes those services that overlap the traditional payment system and the decentralised cryptocurrency ecosystem.

The main characteristics of the **blockchain architecture/technology**, can be described as follows:

- **Permissioned vs permissionless blockchain:** A permissioned blockchain is open source and has a coordinated body, which imposes the number and identity of validators of transactions, which can be limited to private entities or a consortium of institutions; these are also known as private ledgers. A permissionless blockchain is also open source, but does not prescribe or dictate the number and identity of validators of transactions; these are also known as public ledgers.
- **No central point of failure:** Transaction records are stored on multiple decentralised nodes, meaning that the corruption of a single node has no significant effect on the stability or security of the blockchain.
- **Immutability:** The records on the blockchain are unchangeable once they have been approved and recorded. Due to the blockchain architecture having many nodes, every node on the system has a copy of the digital ledger. To add a transaction, each node needs to check its validity and if the majority thinks it is a valid transaction, then it is added to the ledger. Once a transaction is added onto the ledger, no one can just go back and edit it, nor delete it.
- **Consensus mechanisms for transactions validation (Box 2):** The blockchain architecture has two main consensus protocols, which are proof-of-work (PoW) and proof- of-stake (PoS); the latter is used in permissionless protocols to ensure their resilience[38].
- **Trustless architecture:** Anyone can validate transactions in a permissionless blockchain. However, this openness makes them more vulnerable to cyberattacks. It is important to note that proof-of-work networks like Bitcoin have never been successfully hacked and are considered as secure as banks.[39] To attack Bitcoin, someone would need to control 51% of the mining power. This would mean sacrificing the profits from mining just to compromise the network. Proof-of-stake operates on a fundamentally different principle and contains numerous vulnerabilities that can be exploited.
- **Blockchain native tokens**: Native tokens, which include crypto assets, are held by investors who see intrinsic value in their value to be used as collateral for speculative reasons. Furthermore, these tokens are received as a reward for validators of transactions e.g., miners, which derive a certain amount of value from the activity that takes place around the DeFi protocols.

BOX 2: CONSENSUS MECHANISMS IN BLOCKCHAIN

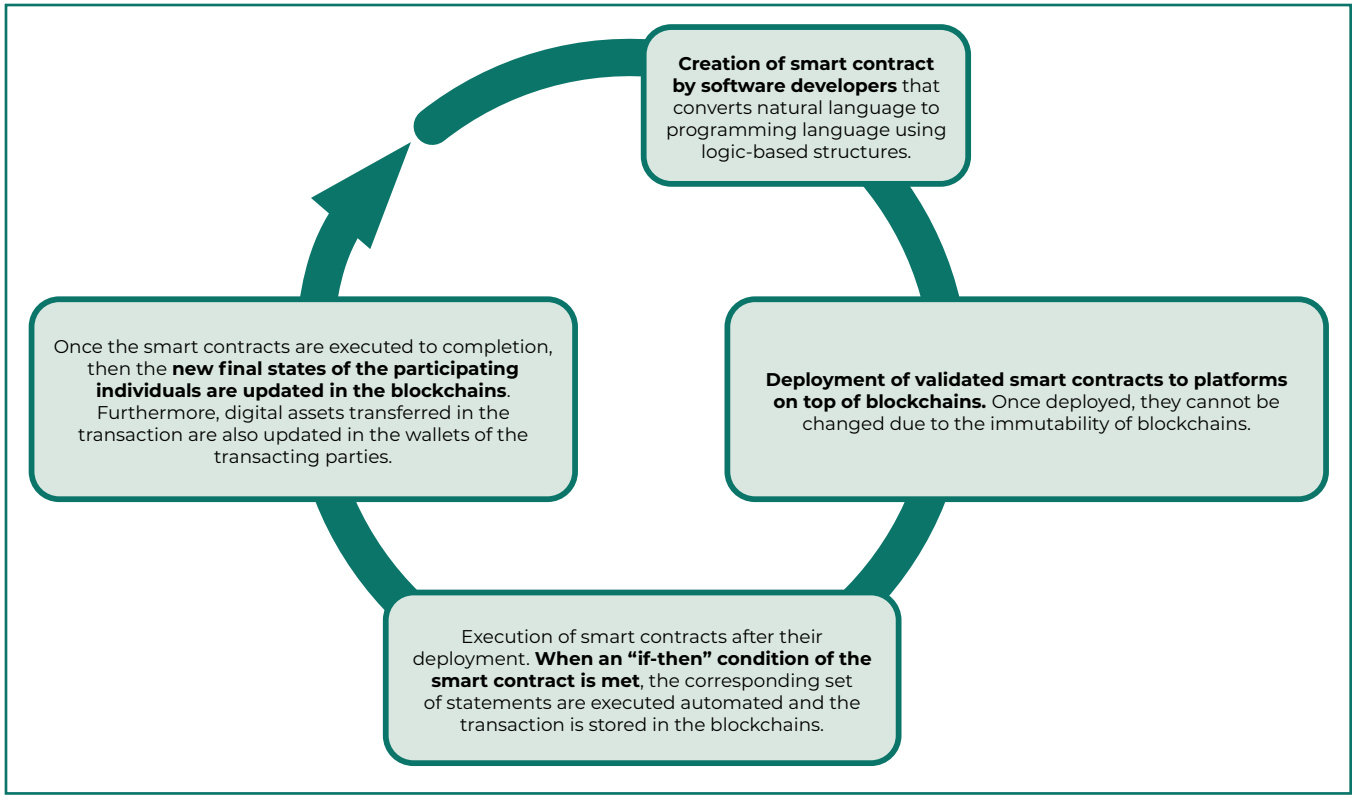
Proof of Work (PoW): In this consensus mechanism for public blockchains, the algorithm rewards the participants who solve cryptographic puzzles to validate transactions and create new blocks, thus the name blockchain. This consensus mechanism requires high levels of computing power and electricity and is believed to be detrimental to the environment due to these requirements.

Proof of Stake (PoS): In this category of consensus mechanism for public blockchains, algorithms depend on a validator's economic stake, or size of deposit, in the network. Therefore, without the computing power and electricity requirements, this consensus mechanism is most promising for a cleaner earther.

[38] BIS (2022), *"Cryptocurrencies and Decentralised Finance"*, available here.
[39] Bitcoin is considered by many a special case; given its size and value, most losses of funds in bitcoin are human error, like loss of private keys.

Smart contracts can be defined as self-executing contracts, with the terms of the agreement directly written into code. In DeFi, smart contracts automate various financial functions, such as lending/borrowing and trading, without the need for intermediaries or traditional third parties. This reduces costs as well as the risk of human error and fraud.

Figure 4: The lifecycle of smart contracts



Source : Kaur, G. et. al. (2023). *"Understanding Cybersecurity Management in Decentralised Finance"*. Springer

Smart contracts have several key characteristics that make them unique and valuable in various applications. These include:

- **Transparency.** All participants of DeFi platforms can view the terms and conditions of the agreement when predefined conditions are met, without the need for intermediaries[40].
- **Immutability.** Once a smart contract is deployed, it cannot be altered, which helps with maintaining trust among the parties involved. Changing the terms of the contract requires the coder to go through the process of obtaining permission from governance token holders of the decentralised autonomous organisation, which can take long and therefore also brings certain risks.
- **Secure.** The use of cryptographic techniques ensures that the contracts are secure and tamper proof[41].
- **Composability.** Composability of smart contracts means that different smart contracts can work together like building blocks. Just like you can combine different Lego pieces to create something new, you can combine smart contracts to create more complex applications. This allows developers to build on existing contracts, adding new features or creating entirely new services without starting from scratch. It makes the DeFi ecosystem very flexible and innovative.

[40] Morgen, D. (2023), *"What Is a Smart Contract? An Overview of Smart Contracts Technology"*, available here.
[41] Investopedia (2024), *"What Are Smart Contracts on the Blockchain and How Do They Work?"*, available here.

- **Tokenisation.** DeFi platforms often tokenise real-world assets, representing them as digital tokens on a blockchain. These tokens can then be traded, lent or borrowed with ease, enabling greater liquidity and accessibility to previously illiquid assets. As a token is a digital asset that is created, issued, and managed on a blockchain; tokenisation naturally follows as a native functionality of the Ethereum blockchain and it is one of the cornerstones of DeFi. Therefore, they are designed to be secure and instantly transferrable, whilst also able to be programmed with a range of built-in functionalities. From real estate security tokens that represent fractionalised properties to platform- specific tokens, which incentivise the use of a particular application, these tokens have proven to be a secure digital alternative for users across the world to access, trade, and store value.

Therefore, the main characteristics of DeFi are as follows:

Non-custodial. This is one of its main defining characteristics. In DeFi applications, no central authority or other intermediary gains access to or control over participants' digital assets; instead, participants manage their private keys, and therefore their digital assets directly[42].

Self-governed and community driven. Most DeFi protocols are open-source and allow the community to review and further develop the code underlying the protocols. In terms of governance, the distribution of governance tokens in many DeFi applications allows users to participate in some decision-making related to the application, depending on the specific arrangements of each application[43].

6.2 INCENTIVE MECHANISMS IN DEFI

Incentive mechanisms in DeFi are essential for attracting and retaining participants, ensuring the smooth operation of protocols, and fostering a robust ecosystem. These mechanisms align the interests of users, developers, and investors, promoting active engagement and network growth.

For investors, one of the primary incentives is the potential for high returns through yield farming and liquidity mining. By providing liquidity to DeFi protocols, investors can earn rewards in the form of additional tokens, significantly boosting their returns. Additionally, DeFi lending platforms allow investors to earn interest on their crypto assets, often at rates higher than those offered by traditional financial institutions. Governance tokens provide investors with voting rights on protocol decisions, aligning their financial interests with the success of the protocol and fostering a sense of community and involvement. The decentralised nature of DeFi also offers greater control and security over investments, as investors retain custody of their assets and can participate in financial activities without relying on intermediaries.

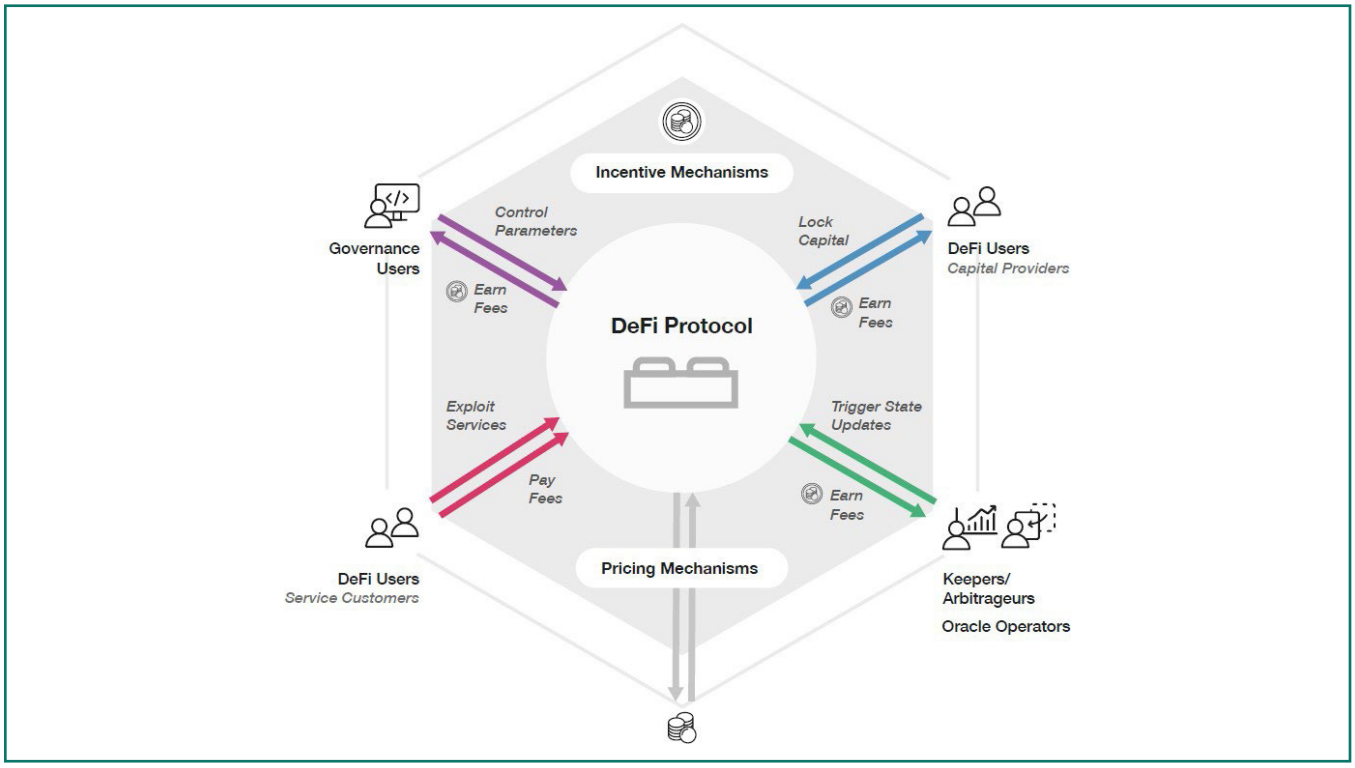
For **developers**, incentives include the allocation of governance tokens, which grant voting rights and a stake in the protocol's decision-making process. This aligns their financial interests with the platform's success. Developers often receive a portion of the transaction fees generated by the platform, providing a continuous revenue stream as the platform grows. Many DeFi projects also set aside a portion of their token supply for developer grants and bounties, rewarding contributions to the codebase, security audits, and feature enhancements.

For **users**, incentives are primarily driven by reduced transaction costs and the ability to participate in financial activities without intermediaries. DeFi platforms often offer lower fees compared to traditional financial services, making them more attractive to users. Additionally, users can benefit from the transparency and security provided by blockchain technology, which ensures that all transactions are recorded and verifiable.

[42] This can be likened to holding assets in a safety deposit box, where the keys make up a DeFi stack and the assets are held in a separate DeFi enabled wallet. A private key is generated when the wallet is created it contains a series of words and numbers that are given to the wallet holder to keep secret so that no one else can access their wallet.
[43] OECD (2022), *"Why Decentralised Finance (DeFi) Matters and the Policy Implications"*, available here.

The BIS highlights that DeFi's architecture can reduce transaction costs by eliminating intermediaries. By removing the need for traditional financial intermediaries such as banks and brokers, DeFi platforms streamline processes and reduce overhead costs. This efficiency is achieved using smart contracts, which automate transactions and reduce the need for manual intervention, thereby lowering operational costs. Figure 5 illustrates the incentive mechanisms within DeFi.

Figure 5: Incentive mechanisms in DeFi



Source: BIS (2023)

6.3 USE CASES OF DEFI

The cornerstone of DeFi is that it uses blockchain and smart contracts to displace the need for financial intermediaries. DeFi use cases are the protocols, which are implemented as executable software programs, i.e., smart contracts, whose execution is automated. This guarantees that these services are reusable and consistent, as the financial functions adhere to the logic outlined in the smart contract itself. As observed in the DeFi architecture (Figure 2), these programs are subsequently deployed on smart contract-enabling DLTs like Ethereum.[44]

Ethereum is a DLT and peer-to-peer network, consisting of various communities and tools that allow individuals to transact and communicate without relying on a central authority or regulatory body. Users within the Ethereum network have control over their data and decide with whom to share it. Since Ethereum is programmable, decentralised applications can be created and launched on its network.[45]

To discuss the DeFi use cases, we need to understand the gaps and challenges of the traditional financial ecosystem that DeFi seeks to address, these include:

- Lack of access to a bank account often resulting in financial exclusion.

[44] BIS (2023), *"The Technology of Decentralised Finance"*, available here.
[45] Ethereum. (2023). *"What is Ethereum?"*. Available here.

- Financial markets that function within certain trading hours and are limited by certain time zones.
- Delayed money transfers due to the need for a traditional third party and exchange rates.

There are numerous DeFi use cases, which are discussed below with some case studies.

For the purposes of this report, we will focus on four use cases, namely payments, lending and borrowing, DEXs, and asset management.

Payments: This is most likely the foundational use case of a DeFi ecosystem and the blockchain ecosystem at large. DeFi platforms enable fast, low-cost, and borderless payments using crypto assets. This can significantly reduce transaction fees and processing times compared to traditional payment systems. DeFi payment solutions are particularly beneficial for cross-border transactions and remittances, providing a more efficient and inclusive financial system[46].

SOUTH AFRICAN EXPERIENCE:

Some fintechs in South Africa are integrating self-custody Web3 wallets into their platforms. Self-custody Web3 is a wallet where users have ultimate ownership of their assets and private keys. This contrasts with custodial wallets where a third party has control, and the user must trust that centralised service. Web3 self-custody wallet can allow users to have access to a secure and streamlined method to swap thousands of tokens across various networks at the best prices, explore a variety of dApps, quickly transfer funds between exchange and wallet, earn yield on their crypto and more, all in one secure wallet.

This innovation has now made it simpler for South African customers to purchase crypto assets from fiat into their wallet and vice versa, through local banking infrastructure[47]. It also allows individual customers to swop their fungible tokens, such as crypto assets, for other fungible tokens. They can also buy, mint, or link their non-fungible tokens to their wallet address.

Lending and borrowing: Lending and borrowing in DeFi involves using blockchain technology and smart contracts to facilitate financial transactions without traditional intermediaries like banks. In DeFi, users can lend their cryptocurrency to earn interest or borrow cryptocurrency by providing collateral. This system operates on decentralised platforms such as Aave and Compound, which use smart contracts to automate and secure transactions.

Lenders deposit their assets into liquidity pools, which are then available for borrowers. Borrowers must provide collateral, often exceeding the loan amount, to secure the loan. This over-collateralisation mitigates the risk for lenders. Interest rates are determined by the supply and demand dynamics within the liquidity pools, and both lenders and borrowers benefit from the transparency and efficiency of the blockchain[48].

[46] IMF BLOG (2021), *"Global Crypto Regulation Should be Comprehensive, Consistent, and Coordinated"*, available here.
[47] Consensys. (2023). *"Banxa and MetaMask Partner to Make it Easier to Access Web3"*. Available here.
[48] CoinMetro (2024), *"DeFi Lending and Borrowing: A Beginner's Guide"*, available here.

SOUTH AFRICAN EXPERIENCE:

Some crypto exchanges are integrating DeFi lending platforms such as Aave into their own platforms and connect lenders and borrowers directly, without the need for intermediaries.

Aave is a DeFi protocol that enables users to lend and borrow cryptocurrencies without the need for a centralised intermediary. It operates as a non-custodial liquidity protocol, allowing participants to act as either suppliers or borrowers.

Suppliers provide liquidity to the market and earn interest, while borrowers can access liquidity by providing collateral[49]. Aave is notable for its flash loans feature, which permits users to borrow assets without collateral for a single transaction, provided the loan is repaid within the same transaction.

The protocol's governance is managed through the AAVE token, which allows token holders to vote on proposals affecting the protocol's development and operations. Security is a priority for Aave, with multiple audits and a bug bounty program in place to identify and mitigate risks.

Decentralised exchanges: DEXs are platforms that allow users to trade crypto assets directly with each other without a central authority. They use blockchain technology and smart contracts to automate and secure transactions, enhancing privacy and control over assets. DEXs offer peer-to-peer trading, increased security, transparency through blockchain records, and greater accessibility since anyone with an internet connection and a crypto asset wallet can use them. Popular DEXs include Uniswap, SushiSwap, and PancakeSwap[50].

SOUTH AFRICAN EXPERIENCE:

Some DEXs are offering customers platforms where they can buy, sell and swap various crypto assets, which include Bitcoin, Ethereum, and others. They emphasise a non-custodial approach meaning that customers retain control over their assets. Further DeFi use cases offered by these DEXs include lending and borrowing as well as trading thereby earning yields through stablecoins and other crypto assets. These platforms further provide customers with tools for tracking market trends and managing crypto asset portfolios, helping customers to make more informed investment decisions.

Asset management: Asset management utilises blockchain technology and smart contracts to manage investments with transparency and efficiency. DeFi platforms offer complete visibility into portfolio performance and composition, enabling real-time asset tracking[51].

Investors maintain control over their funds, while smart contracts automate investment strategies to enhance returns. The composability of DeFi allows for the creation of innovative investment strategies by integrating various financial products[52].

SOUTH AFRICAN EXPERIENCE:

Some fintechs are providing customers with self-custody of their accounts where they can own their assets directly, securely and immutably, and a trading platform for them to trade. This is an example of on-chain CeFi. They also offer their customers direct access to a range of tokenised and investable financial assets, which include bonds[53] and crypto assets where customers participate in the market directly with no financial intermediaries involved. Every investor can get direct access to a range of alternative and private capital investment opportunities through a secure, simple, and flexible capital markets ecosystem.

---

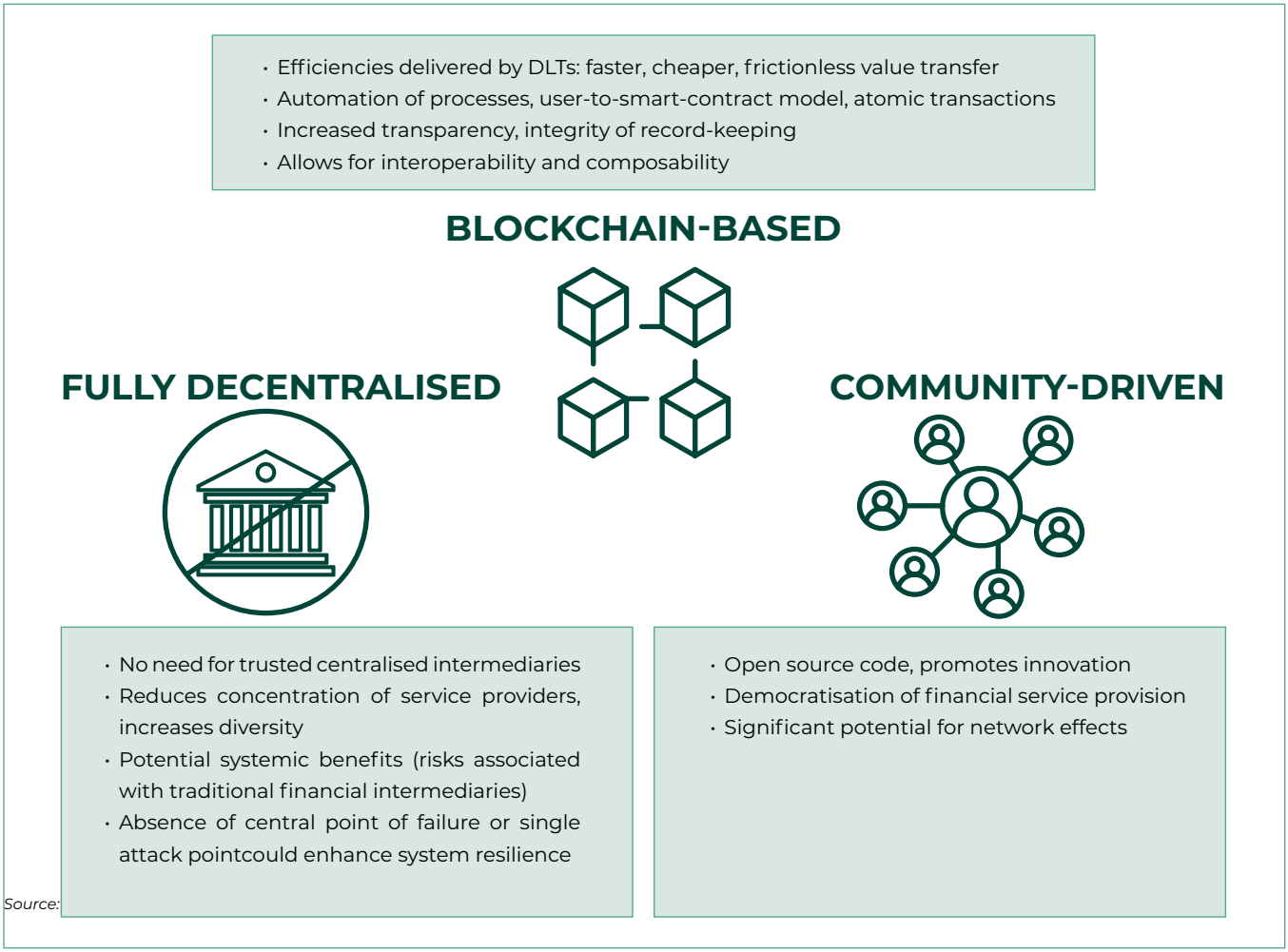
[49] Aave (n.d.), *"Aave documentation"*, available here.
[50] Ethereum.org (n.d), *"Decentralised finance (DeFi)"*, available here.
[51] CoinGecko (2023), *"What is Asset Management in DeFi?"*, available here.
[52] CoinGecko (2023), *"What is Asset Management in DeFi?"*, available here.
[53] IOL (2024), "MeshTrade launches first tokenised corporate bond on the continent", available here.

7. BENEFITS AND RISKS OF DEFI

7.1 BENEFITS OF DEFI

The potential benefits of DeFi are highlighted in Figure 6. The application of DLTs for the provision of financial protocols may reduce some of the risks associated with traditional financial institutions and intermediaries[54]. Increased integration of DeFi with the traditional financial system, could have a beneficial impact on the traditional financial markets, such as stronger competition accompanied by lower transaction costs.

Figure 6: Potential benefits of decentralisation



Source:

One of the most important potential benefits of DeFi is related to financial inclusion and the potential of DeFi to serve underserved parts of the community such as SMMEs. In its ideal form, DeFi could substitute traditional transaction transactional services and overhaul the inflexibility of present processes, allowing SMMEs to tap increased liquidity and alternative credit.

[54] OECD (2022), *"Why Decentralised Finance (DEFI) Matters and the Policy Implications"*, available here.

7.2 RISKS OF DEFI

DeFi presents several risks that regulators need to consider, as illustrated by Table 3.

Table 3: Detailed risks of DeFi

Category	Risk	Details
Operational (software related) risks	Smart contracts	Smart contracts serve as the essential "back-end" software that enables the functionality of a DeFi system. Any flaws in their design, implementation, or upkeep can result in the system not performing as anticipated or intended[55]. Some of the risks of smart contracts include immutability, contractual secrecy, legal enforceability, understandability, and signature verification[56]. Vulnerabilities in smart contracts can enable a malicious attacker to destroy or steal some of the value managed by the contract or enable a situation where this happens as an accidental consequence of an unpredicted sequence of actions[57]. These vulnerabilities include the public availability of the code, which allows hackers to look for bugs or configuration errors that they can exploit to attack the DeFi system and steal or destroy value. Further vulnerabilities are smart contracts that are deployed without adequate review, smart contract immutability, and upgradeable smart contracts, which introduce additional security risks and complications.
	Blockchains	Smart contracts can operate on various blockchain platforms. While there are general risks associated with blockchains, certain risks are unique to the specific characteristics of each blockchain. Blockchain risk is the risk that during DeFi transactions, the base blockchain does not operate properly[58]. There are four ways a blockchain can compromise the functionality of a DeFi protocol deployed on that blockchain, namely: the blockchain stopping its working, blockchain losses of transaction records, lack of correctly executing a smart contract's code. Cybersecurity risks include 51% attacks, Sybil attacks, and distributed denial of service attacks[59].

[55] Enterprise Ethereum Alliance (2024), *"EEA DeFi Risk Assessment Guidelines - Version 1"*, available here.
[56] Kaur, G. et al. (2023), *"Understanding Cybersecurity Management in Decentralised Finance"*, Springer.
[57] Enterprise Ethereum Alliance (2024), *"EEA DeFi Risk Assessment Guidelines - Version 1"*, available here.
[58] Enterprise Ethereum Alliance (2024), *"EEA DeFi Risk Assessment Guidelines - Version 1"*, available here.
[59] Kaur, G. et al. (2023), *"Understanding Cybersecurity Management in Decentralised Finance"*, Springer.

	Oracle risk	Oracles are automated information sources that originate outside the blockchain where they are used. The sources and usage of this information can introduce additional risks, especially due to the centralisation aspect of oracles. These risks include potential issues with data accuracy and manipulation, which can affect the information provided to smart contracts. Additionally, relying on a limited number of or insecure data sources can create a single point of failure, where manipulation or malfunctioning of the oracle can have significant negative impacts. Governance and upgradability are also concerns[60].
	Bridge[61] risk	Bridges facilitate interactions between multiple blockchains. Besides software risks, they face market risks that affect the relationship between the blockchains. Due to the significant value, they can hold or transfer, they are appealing targets for hackers. The primary risks with a traditional bridge include counterparty risk, where users rely on bridge operators to consistently process transactions and safeguard funds, avoiding theft or loss (custodial risk).
Consumers	Lack of consumer protection	DeFi operates in a largely unregulated environment, which means there are fewer protections for consumers compared to traditional financial systems. Consumers may have limited recourse mechanisms in cases of fraud, platform failure, or loss of funds[62].
	Custodial risk	Custodial risk arises because mistakes or malicious behaviour can result in loss or theft if access to a private key is lost or stolen (a person's digital wallet can be hacked to obtain an individual's private key)[63].

[60] Enterprise Ethereum Alliance (2024), *"EEA DeFi Risk Assessment Guidelines - Version 1"*, available here.
[61] Bridges in blockchain are like connectors that allow different blockchains to communicate and share information with each other. Imagine you have two separate islands (blockchains) with their own unique resources (tokens and data). A bridge helps transfer these resources from one island to the other, enabling them to work together. This is important because it allows users to move their assets across different blockchains, take advantage of various features, and participate in multiple blockchain ecosystems without being limited to just one. Bridges enhance the interoperability and flexibility of blockchain networks, making the entire system more versatile and efficient.
[62] Mitchell, R. (2022), *"DeFi-ing the Rules: Five Opportunities and Five Risks of Decentralised Finance"*, available here.
[63] Enterprise Ethereum Alliance (2024), *"EEA DeFi Risk Assessment Guidelines - Version 1"*, available here.

Market risks	Market manipulation	The decentralised and open-access nature of DeFi can make it susceptible to market manipulation by hackers[64]. Without centralised oversight, bad actors can exploit price manipulation tactics, such as pump-and-dump schemes[65, 66].
	Liquidity risks	DeFi platforms often rely on liquidity pools, which can be volatile. Sudden withdrawals or market shocks can lead to liquidIty shortages, affecting the stability of the platform and potentially leading to losses for consumers.
	Interoperability challenges	DeFi platforms often interact with multiple blockchain networks and protocols. Interoperability issues can arise, leading to transaction failures or security vulnerabilities[67].
	Financial stability risks	As DeFi grows, its interconnectedness with traditional financial systems increases. This can amplify vulnerabilities and pose risks to overall financial stability[68].
Standards conformance risks	Lack of standardisation	The absence of standardisation in DeFi datasets and codebases complicates the processes of data collection, reconciliation, and analysis across various protocols, blockchains, and markets. Data providers may employ significantly different methodologies for data aggregation and metric calculation. Furthermore, there is a lack of uniformity in the code used to develop DeFi protocols, exacerbating these challenges.
	Operational accounting risks	Operational accounting risks stem from errors in accounting processes: Discrepancies between on-chain positions and reported financial positions can occur if open positions, like liquidity pool tokens staked in a protocol, are not properly accounted for[69].

[64] The strength and integrity of the DeFi system relies on the strength and integrity of the underlying software, and leaves DeFi offerings vulnerable to software attacks, for example:

- Oracle manipulation: Attackers exploit weaknesses in the price feeds that DeFi protocols rely on. By providing incorrect price data, they can artificially inflate or deflate the value of an asset, creating profitable arbitrage opportunities.
- Flash loan attacks: These allow users to borrow large amounts of cryptoassets without collateral, provided the loan is repaid within the same transaction. Attackers use these loans to manipulate asset prices in liquidity pools, which oracles then use to determine prices, leading to incorrect pricing data being fed into DeFi protocols.
- Additionally, some smart contracts calculate token prices based on supply and demand within the contract. Attackers can manipulate these calculations by temporarily altering the token supply using flash loans, causing the smart contract to misprice the asset.
- Insufficient input validation: attackers manipulate the parameters passed to the contract, including altering price data or other critical inputs, leading to incorrect valuations and potential exploitation.

[65] A pump-and-dump scheme in DeFi involves manipulating the price of a token to artificially inflate its value before selling off large quantities at the peak price. It works through (i) the promotion of a token by a group of actors, who often use false claims and create a sense of urgency to attract investors, (ii) price inflation through prices rising sharply as more investors buy into the token, (iii) dumping as the manipulators sell off their holdings at the inflated price thereby making a significant profit, and (iv) crashing as the price of the token plumets leaving the investors with significant loses,

[66] Rodrigues, F. (2024), *"DeFi pump-and-dump schemes rake in millions, harm industry credibility"*, available here.

[67] Wolfson, R. (2024), *"Blockchain Projects Tackle DeFi's Biggest Hurdle: Consumer Confidence"* available here.

[68] Wolfson, R. (2024), *"Blockchain Projects Tackle DeFi's Biggest Hurdle: Consumer Confidence"* available here.

[69] Enterprise Ethereum Alliance (2024), *"EEA DeFi Risk Assessment Guidelines - Version 1"*, available here.

Compliance and legal risk	Pseudonymity	A significant challenge to data analytics is the pseudonymous nature of on-chain transactional data and the lack of transparency in off-chain data. This opacity is often intensified by market participants employing multiple pseudonymous addresses to obscure their activities. Consequently, this creates difficulties in evaluating aspects such as retail investor participation levels, market concentrations, interconnectedness within DeFi or with the broader financial ecosystem, and risks associated with specific market participants or activities[70]. This presents AML/CFT risks.[71].

These attacks highlight the importance of robust security measures, such as using decentralised oracles, implementing time-weighted average prices (TWAP), and conducting thorough security audits to protect DeFi protocols from manipulation. Addressing these risks requires a balanced regulatory and supervisory approach that fosters innovation while ensuring consumer protection and fair market conduct.

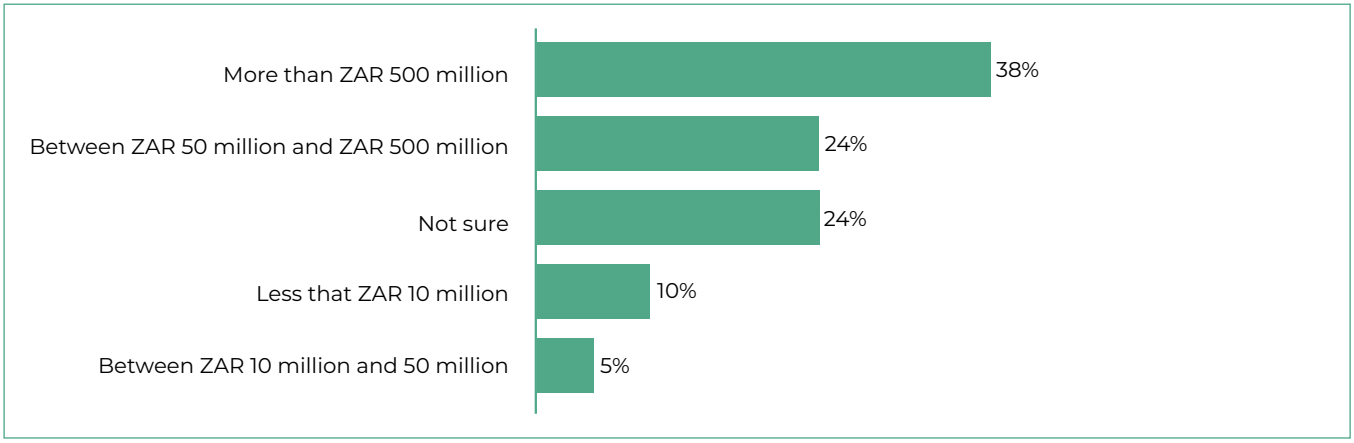
[70] IOSCO (2023), *"Final Report with Policy Recommendations for Decentralised Finance (DeFi)"*, available here.
[71] Enterprise Ethereum Alliance (2024), *"EEA DeFi Risk Assessment Guidelines - Version 1"*, available here.

8. VIEWS FROM MARKET PARTICIPANTS

Twenty-one crypto asset service providers in South Africa responded substantively to the FSCA's survey. Our survey revealed South Africa's growing interest in Defi activities, despite its challenges.

8.1 DEFI TOTAL VALUE LOCKED IN SOUTH AFRICA

Figure 7: Expected DeFi total value locked in South Africa



Measuring the size of DeFi participation includes identifying the currency value of crypto assets that are so-called "locked" in smart contracts on a particular blockchain. The majority of the respondents estimated that the DeFi TVL is more than R500 million (38%), followed by the range between R50 million and R500 million and a range that selected "Not sure", which are both at 24%. This is then followed by those who estimated the DeFi TVL at less than R10 million in South Africa at 10%.

These market views paint a picture of DeFi market that is still in a nascent stage, but growing. Media reports indicate that South African crypto asset exchanges are increasingly introducing DeFi tokens on their platforms. They are seeing a heightened appetite from the local market to embrace DeFi coins, which are growing in popularity globally.

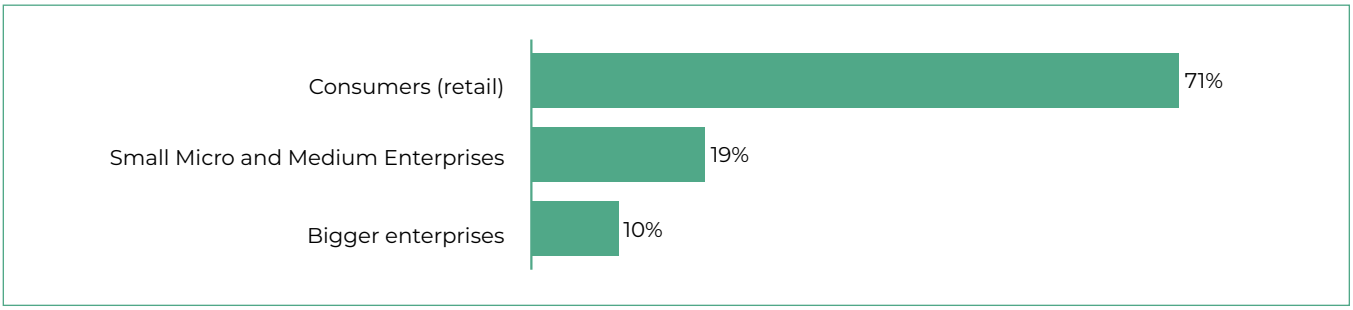
In February this year, one leading crypto exchange in the country announced that it had added three new crypto assets to invest in and that these assets are leading in DeFi[72]. Moreover, the DeFi market in South Africa is projected to reach approximately US$115.6 million in 2024. This market is expected to grow at an annual rate (CAGR) of 11.82%, reaching around US$180.7 million by 2028[73].

Although DeFi market size is still very small compared to the traditional financial sector, it is imperative for the FSCA to continuously monitor the sector for any risks that might be detrimental to consumers' welfare.

[72] IT Web (2024), "*SA crypto players diversify portfolios with DeFi coins*", available here.
[73] Statista (2024), "*DeFi - South Africa*", available here.

8.2 DEFI CUSTOMER TYPE

Figure 8: Most likely customer type for DeFi financial services offerings

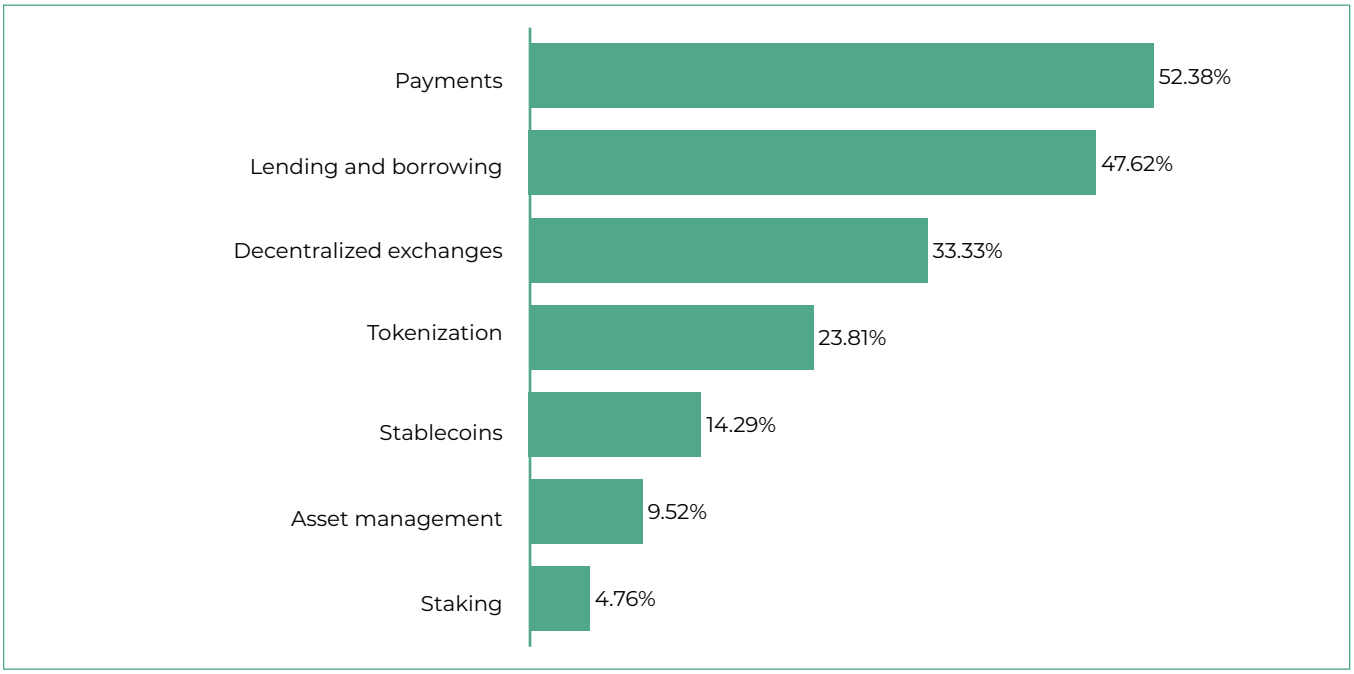


Of the surveyed participants, 71% stated that the most likely type of customer for DeFi financial services offerings is the retail customer, followed by SMMEs at 19% and lastly by bigger enterprises at 10%. Due to the complexity of DeFi protocols, the current ecosystem seems to primarily cater to retail investors who are crypto/tech savvy and have a high-risk appetite.

Educating consumers about the risks and benefits of DeFi can empower them to make informed decisions and providing resources and tools to help users understand how to safely interact with DeFi platforms is essential[74].

8.3 KEY USE CASES OF DEFI

Figure 9: Key use cases arising from DeFi



According to the survey, market participants identified multiple prominent use cases of DeFi in South Africa, including payments (52%), lending and borrowing (48%), and decentralised exchanges (33%). The foundational use case of DeFi is payments, as from the introduction of crypto assets through Satoshi Nakamoto, which was to facilitate borderless payments without an intermediary or third party

[74] Unlike many TradFi products and services that provide clear disclosure statements regarding their features, risks, and costs in plain language, as required by law, the nascent and technically complex nature of DeFi protocols can be difficult for an average retail investor to fully comprehend.

involved. The use of crypto assets and stablecoins is what enables delivery vs payment in the many DeFi protocols.

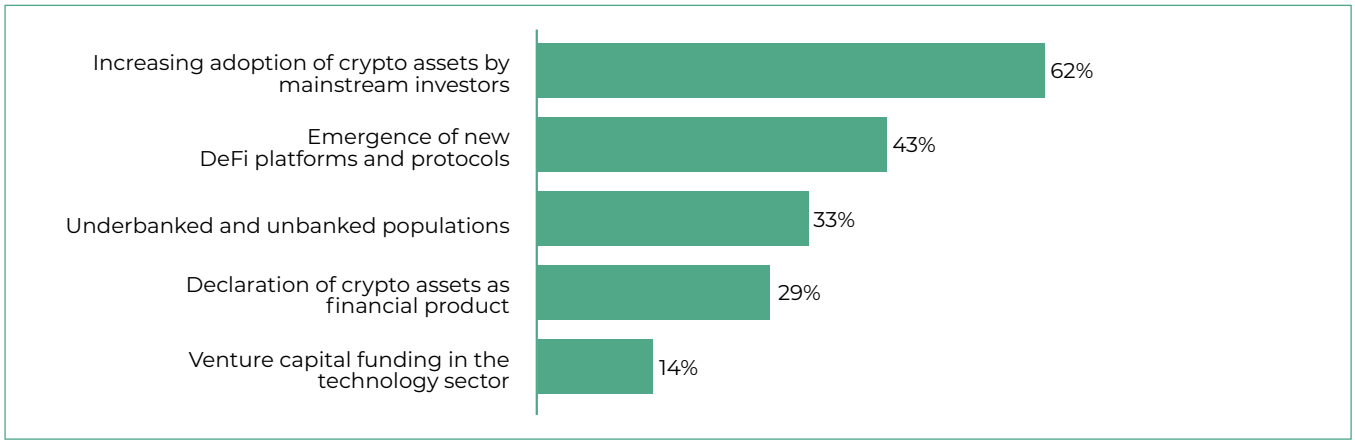
DeFi payment solutions have the potential to foster a more inclusive economic system for underbanked and unbanked communities, while also aiding large financial institutions in optimising market infrastructure and enhancing services for both wholesale and retail clients[75]. Global trends show that lending and borrowing, and decentralised exchanges, tokenisation, and stablecoins are the other leading use cases in DeFi[76].

To build understanding of the DeFi landscape and inform regulatory and supervisory responses, the FSCA should consider analysing activities and arrangements of the DeFi protocols, and identify risks associated with prioritised use cases

8.4 FUTURE DRIVERS OF DEFI

The leading future drivers of DeFi identified by respondents include the adoption of crypto assets by mainstream investors (62%) and the emergence of new DeFi platforms and protocols (43%). The percentages reflect that respondents could select more than one option; hence the total exceeds 100%. This view is in line with global developments that show stablecoins being critical elements for DeFi growth. The Bank for International Settlements (BIS) highlighted that stablecoins (See Box 3) play a crucial role in bridging the crypto asset and TradFi markets, allowing DeFi market participants to avoid frequent conversion to and from fiat currency and facilitating fund transfers across platforms and between users (BIS, 2021).

Figure 10: Future drivers of DeFi.



BOX 3: STABLECOINS IN DEFI

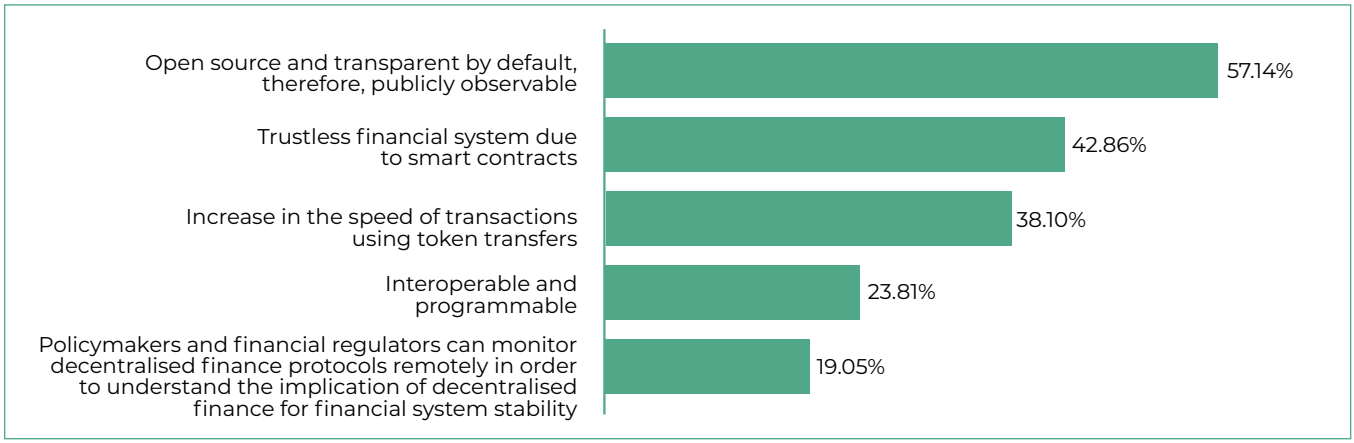
Stablecoins are a stable and liquid form of crypto-asset, which helps to solve the issue of price volatility of crypto-assets, thereby enhancing the functionality of DeFi protocols. Concurrent with the growth of the global DeFi market, stablecoins have experienced exponential growth since June 2020 with a total market capitalisation of US$151 billion at the end of March 2024. Moreover, the availability of decentralised lending, borrowing, and trading platforms are contributing to the growth of DeFi, allowing users to interact with financial markets in a more decentralised and permissionless way.

[75] consensys (2024), *"Blockchain for Decentralised Finance (DeFi)"*, available here.
[76] EMURGO (2023), *"The 5 Most Promising Real Use Cases for DeFi"*, available here.

Looking into the future, the DeFi market is expected to continue growing. Factors that are expected to drive this growth include the ongoing development of new DeFi use cases and applications, the increasing adoption of crypto assets by mainstream investors, and the continued emergence of new DeFi platforms and protocols.

8.5 KEY OPPORTUNITIES ARISING FROM DEFI

Figure 11: Opportunities arising from DeFi



Key opportunities arising from DeFi include an open source and transparent by default, and therefore, publicly observable financial system (57%) and secondly, a trustless financial system due to smart contracts (43%). This will increase consumer trust in the financial system.

DeFi is designed for transparency, with all transactions recorded on the blockchain. This can improve the visibility of financial transactions, reduce fraud risk, and enhance trust in the system[77]. Additionally, DeFi services operate through smart contracts and transparent protocols, ensuring automatic execution and recording according to predefined rules, thus eliminating intermediary or custody risks[78]. Lastly, using the Ethereum blockchain as an example, we observe faster transaction speeds with tokens, as Ethereum can handle nearly 119 transactions per second at maximum theoretical transaction per second (TPS)[79], while centralised systems can process thousands of transactions at a similar level[80]. These opportunities should be explored in detail by the FSCA as part of its future research.

8.6 POTENTIAL OUTCOMES OF DECENTRALISED FINANCE

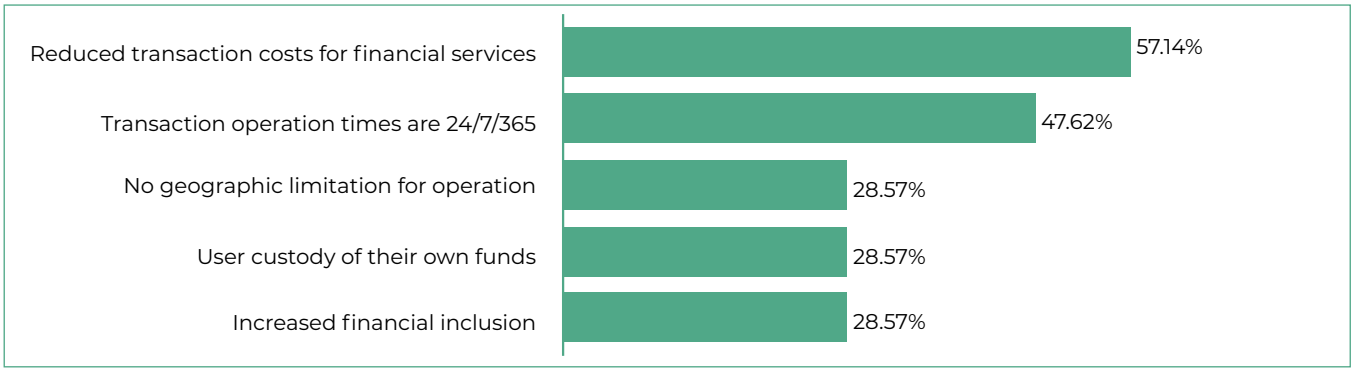
A key outcome of DeFi may be the potential to reduce transaction costs for financial services (57%), like the traditional financial system, there are several layers where rents can accumulate due to endogenous constraints to competition of transaction costs[81]. Secondly, other potential outcomes of DeFi include transaction operation times that are 24/7/365 (48%), and no geographic limitation for operation (29%) as customers only need an internet connection to participate in DeFi financial services.

However, blockchain-based DeFi may not generate immediate and real benefits to users in South Africa if challenges remain related to regulatory uncertainty regarding Defi protocols, digital illiteracy

[77] Finance Magnates (2023), *"The Promise of DeFi: Use Cases, Opportunities, and Risks"*, available here.
[78] EUROFI (2022), *"Decentralised Finance (DeFi): Opportunities, Challenges and Policy Implications"*, available here.
[79] Chainspect (2024), *"What is Transactions Per Second (TPS)?"*, available here.
[80] Jia, D.W. (2022), *"DeFi's Pros and Cons: Opportunities and Challenges"*, available here.
[81] BIS (2022), *"Cryptocurrencies and Decentralised Finance"*, available here.

among a large segment of the population and heightened levels of cyber crime. Wide-spread adoption will likely then be similarly curtailed.

Figure 12: Potential DeFi outcomes

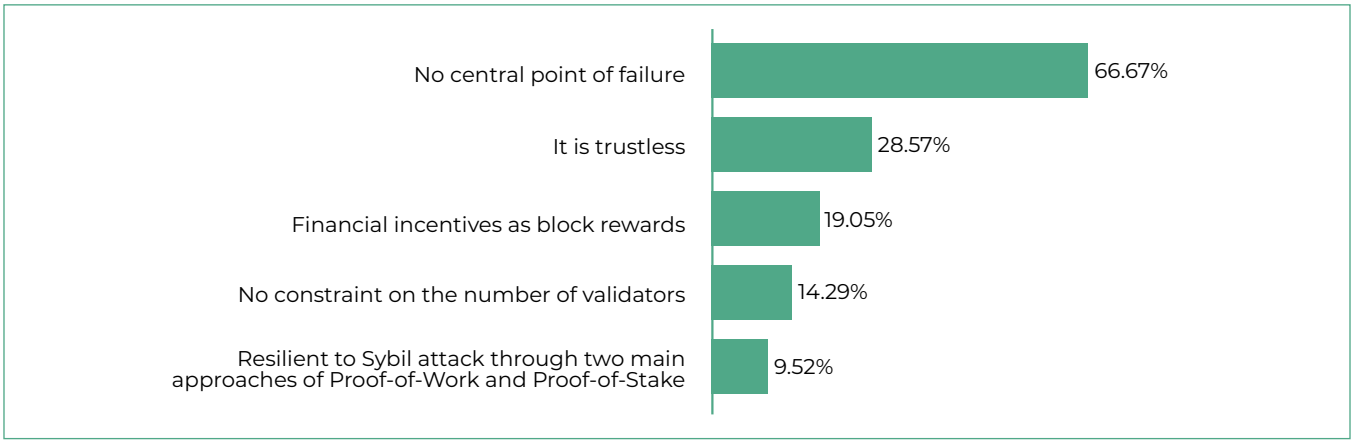


8.7 ADVANTAGES OF PERMISSIONLESS BLOCKCHAIN TECHNOLOGY

Key identified advantages of permissionless blockchain technology include no central point of failure (67%) and that it is trustless (29%). These advantages contribute to firming up the security of blockchain technology. However, it isn't without its vulnerabilities, as illustrated in Figure 14.

As covered earlier in this report, permissionless blockchains offer significant advantages for DeFi, including enhanced security and reliability due to the absence of a central point of failure. Their trustless nature ensures transaction integrity without needing participants to trust each other or a central authority. Financial incentives like block rewards encourage network maintenance and security. Additionally, the unlimited number of validators promotes inclusivity and decentralisation. These blockchains are also resilient to Sybil attacks through proof of work (PoW) and proof of stake (PoS) mechanisms, making them a robust foundation for secure, inclusive, and trustless DeFi applications.

Figure 13: Advantages of permissionless blockchain technology



8.8 KEY RISKS OF DEFI

The main risks of DeFi identified in the survey include the execution of smart contracts resulting from coding errors when forming smart financial contracts (43%) and the interconnectedness or dependency risk as DeFi protocols allow various smart contracts and decentralised blockchain applications to interact with each other to offer new services based on a combination of existing ones (33%).

Feedback from the market participants confirms the view that DeFi ecosystem has structural flaws and poses risks that might potentially undermine consumer protection and market integrity. Additionally, the bear market faced in 2022 — commonly referred to as the "crypto winter" — revealed that DeFi ecosystem displays many of the vulnerabilities associated with the traditional financial system (TradFi), such as governance, operational weaknesses, liquidity and maturity mismatches, leverage and interconnectedness[82].

Going forward, the FSCA will consider testing certain DeFi use cases in the Regulatory Sandbox of the Intergovernmental Fintech Working Group (IFWG). This will deepen the FSCA understanding of the potential risks emanating from DeFi activities and informing an appropriate regulatory and supervisory response.

Figure 14: Vulnerabilities of DeFi in the financial sector

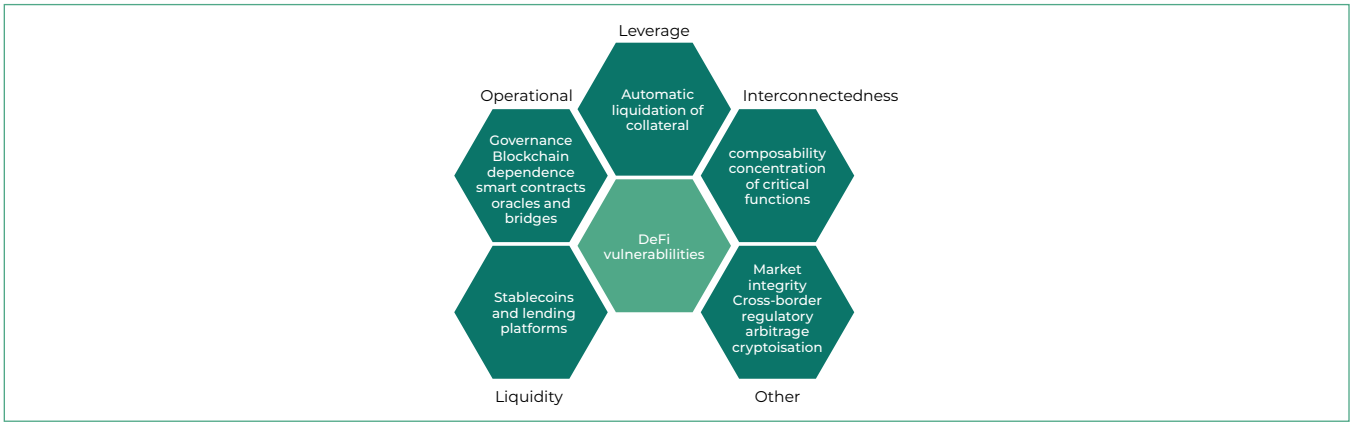
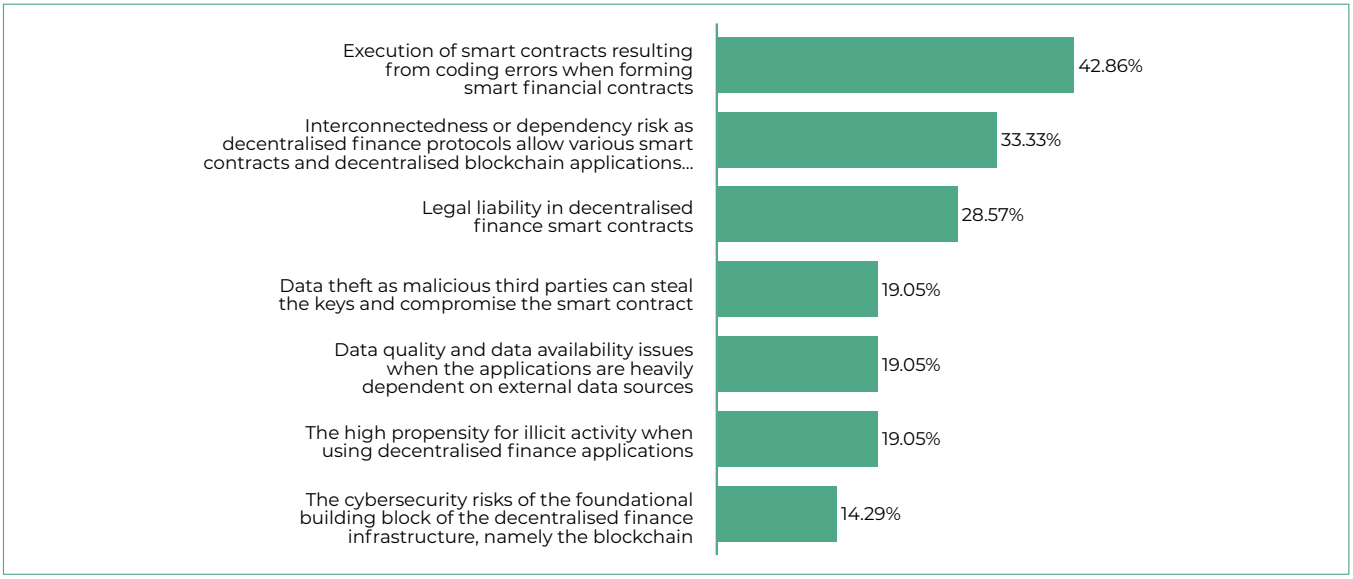


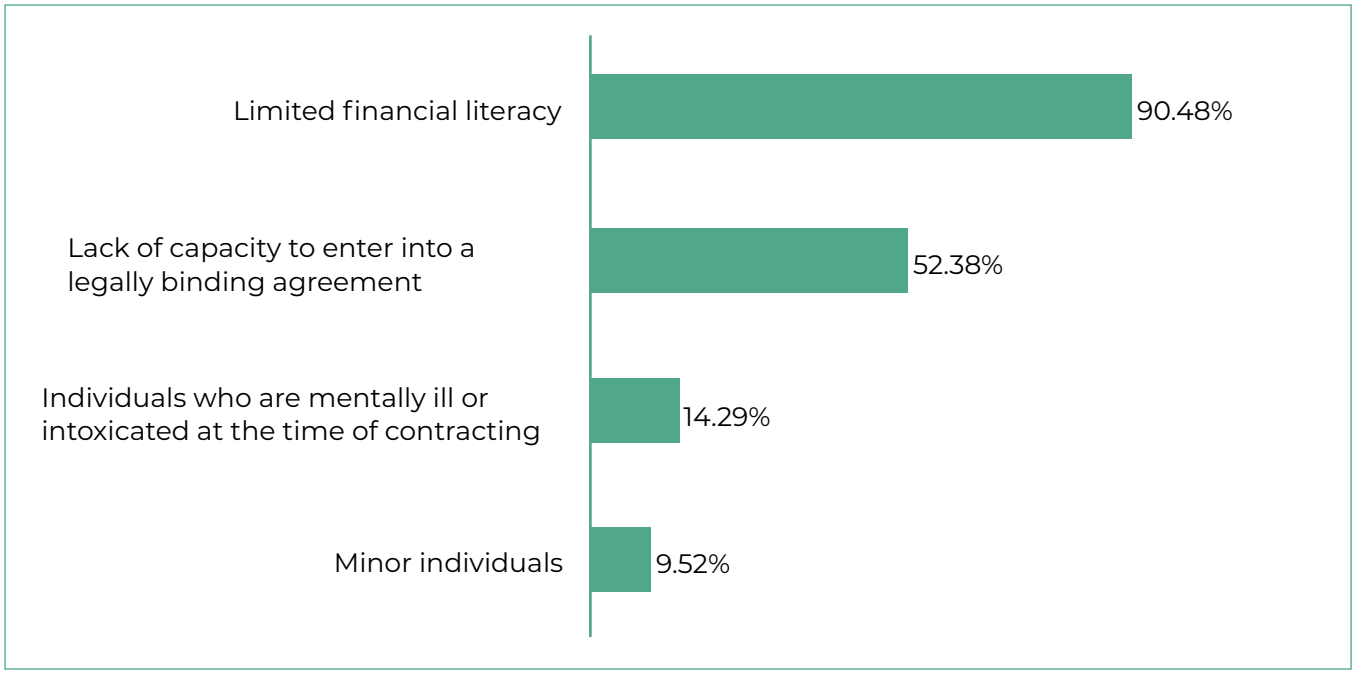
Figure 15: Key risks of DeFi



[82] Globally there is a market practice that anyone using DeFi protocols should review the report of the auditors of the smart contract and ensure that the report includes the actions taken for the developers of the smart contract to address the findings.

8.9 CONSUMER PROTECTION CONSIDERATIONS WITH SMART CONTRACTS

Figure 16: Consumer protection considerations with smart contracts specific to user competence



When it comes to consumer protection considerations with smart contracts, the main themes that arose in the survey were that consumers could be exposed due to limited financial literacy (90%), lack of capacity to enter into a legally binding agreement (52%), and individuals who are mentally ill or intoxicated at the time of contracting (14%).

When considering consumer protection in the context of smart contracts, several important aspects must be addressed. One key concern is limited financial literacy. Many consumers may not fully understand the technical and financial implications of smart contracts, leading to potential exploitation or unintended commitments. Additionally, there is the issue of capacity to enter into a legally binding agreement. Individuals who lack the legal capacity, such as minors or those with cognitive impairments, may inadvertently enter smart contracts without fully comprehending their obligations.

Furthermore, the protection of individuals who are mentally ill or intoxicated at the time of contracting is crucial. These individuals may not be able to make informed decisions, raising questions about the enforceability and fairness of such agreements. Addressing these concerns requires robust legal frameworks and consumer education to ensure that smart contracts are used ethically and responsibly[83, 84, 85]. However, this will be a complex approach for the FSCA to achieve given the international nature of DeFi.

[83] Forbes, L. (2022), *"Consumer Protection in the Face of Smart Contracts", Loyola Consumer Law Review 34 (1)*, available here.
[84] Kwick Attorneys (N.D.), *"Smart Contracts and Legal Enforceability: A Detailed Analysis"*, available here.
[85] Forbes, L. (2023), *"Consumer Protection in the Face of Smart Contracts"*, available here.

9. IS DEFI TRULY DECENTRALISED?

DeFi is not without its risks. The decentralised nature of DeFi platforms introduces several vulnerabilities that can impact their stability and security. These risks include smart contract vulnerabilities, oracle risks, custodial risks, and regulatory challenges[86]. While the main vision of DeFi is intermediation without centralised entities, there is an argument to be made that some form of centralisation is inevitable[87]. The Bank for International Settlements (BIS) has highlighted the *"decentralisation illusion"* in DeFi, noting that the need for governance inevitably introduces some level of centralisation. Structural aspects of DeFi, such as the consensus mechanisms used in blockchain networks, tend to concentrate power rather than distribute it evenly[88]. This also points out that DeFi's vulnerabilities, including high leverage, liquidity mismatches, and interconnectedness, can pose significant risks to financial stability. These vulnerabilities are exacerbated by the lack of traditional financial shock absorbers, such as banks, which can provide liquidity during times of stress[89].

Many DeFi projects are developed and maintained by a small group of developers or a single organisation, which can hold significant influence over the project's direction and governance[90]. Governance tokens, intended to distribute control, can often be concentrated in the hands of early investors and insiders, leading to a centralisation of power. Additionally, DeFi platforms depend on existing blockchain networks like Ethereum, where centralisation issues such as node distribution and control by large stakeholders can impact the decentralisation of the applications built on these networks.

Liquidity provision in DeFi markets is another area where centralisation can occur. A few large liquidity providers often dominate these markets, giving them the ability to influence market dynamics and prices. Furthermore, as DeFi continues to grow, it attracts regulatory attention. Compliance with regulations may necessitate the implementation of centralised controls, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures, which can further erode the decentralised nature of these platforms.

Price oracles, which provide external data to smart contracts, are another centralising element in DeFi. These oracles are often controlled by a limited number of entities, and their accuracy and reliability are crucial for the proper functioning of DeFi applications. If an oracle is compromised or manipulated, it can have significant repercussions across the DeFi ecosystem, highlighting a point of centralisation that can undermine the system's integrity.

Governance in DeFi also presents centralisation challenges. While decentralised autonomous organisations (DAOs) aim to distribute governance more equitably, the reality is that governance tokens can be unevenly distributed. This concentration of tokens allows a small group of holders to exert disproportionate influence over decision-making processes, which can lead to centralisation of control[91].

The question of whether centralisation in DeFi is inherently negative is nuanced and depends on various factors. Centralisation can introduce both benefits and risks to the DeFi ecosystem. On the one hand, centralisation can enhance efficiency and speed, as centralised systems can process transactions faster and more efficiently than decentralised ones. This is because decision-making and transaction validation are handled by a smaller number of entities, reducing the time and computational resources required.

---

[86] VISTRA (2022), *"Decentralised finance: Understanding the benefits, risks and challenges of DeFi"*, available here.
[87] BIS (2021), *"DeFi risks and the decentralisation illusion"*, available here.
[88] Business Insider (2021), *"The decentralisation promised by DeFi is an 'illusion' and a threat to global financial stability, BIS warns"*, available here.
[89] VISTRA (2022), *"Decentralised finance: Understanding the benefits, risks and challenges of DeFi"*, available here.
[90] Enterprising Investor (2022), *"DeFi-ing the Rules: Five Opportunities and Five Risks of Decentralised Finance"*, available here.
[91] BIS (2021), *"DeFi risks and the decentralisation illusion"*, available here.

Additionally, centralised control can facilitate regulatory compliance, making it easier for DeFi platforms to adhere to requirements such as KYC and AML procedures. This can enhance the legitimacy and acceptance of DeFi platforms in the broader financial system. Furthermore, centralised entities can implement robust security measures and provide a level of stability that might be harder to achieve in a fully decentralised system, allowing them to act quickly to address vulnerabilities or breaches.

On the other hand, centralisation introduces significant risks. It can create single points of failure, where the compromise of a central entity can have widespread repercussions across the entire system, undermining the resilience that decentralisation aims to provide. Centralised control can also lead to a concentration of power among a few entities, which can influence decision-making processes and potentially act in their own interests rather than those of the broader community. This concentration of power can erode the core principle of DeFi, which is to eliminate the need for trust in intermediaries. Despite these challenges, the DeFi ecosystem is evolving, with efforts underway to address centralisation concerns. Innovations like decentralised autonomous organisations (DAOs) aim to distribute governance more equitably, and alternative blockchain networks and Layer 2 (L2) scaling solutions are being explored to reduce reliance on any single infrastructure. While DeFi holds the potential for significant decentralisation, various factors contribute to centralisation within the ecosystem, making the reality more nuanced.

10. CONCLUSION

If South African DeFi evolves in a way that protects consumers and builds trust, it could support competition and financial inclusion, decreasing dependence on traditional financial intermediaries. However, it introduces significant risks. Vulnerabilities in smart contracts and other supporting software and systems, as well as inter-operability challenges, may expose users to fraud, misrepresentation and cyber security threats, while also opening the market to manipulation. User mistakes or malicious behaviour can expose consumers to theft if access to a private key is lost or stolen. Market shocks can drain liquidity pools, effecting the stability of the platform.

While DeFi is fundamentally characterised by its decentralised nature, elements of centralisation still exist within the ecosystem. These elements can manifest in various forms, such as centralised governance structures, reliance on centralised oracles, and the concentration of power among a few key developers or entities. Recognising these centralisation aspects is crucial for understanding the full scope of DeFi's impact and the associated risks, particularly from a consumer protection and market conduct perspective.

From a consumer protection standpoint, the presence of centralisation within DeFi can lead to potential conflicts of interest, lack of accountability, and increased vulnerability to fraud and manipulation. Ensuring robust consumer protection measures, such as transparency requirements, regular audits, and dispute resolution mechanisms, is essential to safeguard users against these risks.

In terms of market conduct, centralisation elements can undermine the principles of fair and transparent markets. It is important to implement regulatory measures that promote fair treatment of consumers, prevent market manipulation, and ensure that DeFi platforms operate ethically and transparently. This includes enforcing compliance with anti-money laundering (AML) and counter- terrorism financing (CTF) regulations, as well as promoting best practices in governance and operational standards.

A robust and adaptive regulatory environment for DeFi that safeguards the interests of consumers, and the financial system will rely on stakeholder engagement and participation. Public–private dialogue and collaboration could for example help address concerns about blockchain technology and the latest developments in international regulatory standards. Formal reviews, such as consultative documents and regulatory sandboxes, could solicit the views of market participants and ensure that regulatory authorities and stakeholders are aligned and that decision-making processes are transparent. Alternatively, knowledge exchange activities, such as workshops, seminars and conferences, could provide regulators with the opportunity to clarify regulatory expectations and allow market participants to share their views and concerns regarding DeFi applications.

LIST OF ABBREVIATIONS AND ACRONYMS

ACRONYM	FULL TERM
AML	Anti-Money Laundering
BIS	Bank for International Settlements
CeFi	Centralised finance
CEX	Centralised exchange
CTF	Counter-terrorism financing
DAO	Decentralised autonomous organisation
dApp	DeFi application
DeFi	Decentralised finance
DEX	Decentralised exchange
DLT	Distributed ledger technology
ETH	Ethereum
FTX	Futures Exchange
IOSCO	International Organisation of Securities Commissions
KYC	Know your customer
KYT	Know your transaction
NFT	Non-fungible token
PoS	Proof of stake
PoW	Proof of work
TCF	Treat Customers Fairly
TradFi	Traditional financial system
TVL	Total Value Locked

GLOSSARY

TERM	DEFINITION
51% attack	When a malicious actor can compromise more than half of the validators on the network, the actor can execute fraudulent transactions.
Blockchain	A form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerised process by which transactions are validated.
Centralised exchange	A crypto-asset trading platform that facilitates the buying and selling of crypto-assets, either for fiat currencies, or for another digital asset. The platform functions as an intermediary and sometimes provides custody and other services.
Centralised finance	Centralised intermediaries (for example lending or trading platforms) within the crypto-asset ecosystem that purport to offer some of the features of DeFi with some of the ease of use and security of traditional financial-services products.
Composability	A blockchain is composable if it allows developers to easily build innovative decentralised applications (dApps) and cross-chain protocols.
Consensus mechanism	In DLT applications, the process by which validators agree on the state of a distributed ledger.
Crypto asset	A digital representation of value that – • is not issued by a central bank, but is capable of being traded, transferred or stored electronically by natural and legal persons for the purpose of payment, investment and other forms of utility. • applies cryptographic techniques; and • uses DLT.
Cryptography	The conversion of data into private code using encryption algorithms, typically for transmission over a public network.
Decentralised Autonomous Organisation	In theory, a decentralised application consisting of rules of operation that dictate who can execute a certain behaviour or make an upgrade. Code helps create an organisational structure intended to function without a centralised management structure.
Decentralised Applications	DeFi applications offering services such as lending or trading, predominantly between crypto assets including stablecoins.
Decentralised finance	A set of alternative financial markets, products and systems that operate using crypto-assets and 'smart contracts' (software) built using distributed ledger or similar technology.
DeFi protocol	A DeFi protocol provides one or more financial services to economic agents. Financial services are implemented as program functions by one or more smart contracts.
Digital asset	A digital representation of value, which can be used for payment or investment purposes or to access a good or service.

TERM	DEFINITION
DLT	A means of saving information through a distributed ledger, i.e. a repeated digital copy of data available at multiple locations.
Governance tokens	Tokens issued as an incentive, allowing the user the purported opportunity to become a partial owner and decision-maker in a DeFi protocol.
DeFi Liquidity pool	A smart contract that locks in a certain amount of digital assets to facilitate its underlying economic activity (e.g. trading or lending) to take place.
Native token	The base token of a blockchain which plays an integral part of the operation of the protocol it is issued on and that is created at its genesis. It is usually used to pay transaction fees.
Oracle	A service that enables smart contracts to access, in real-time, relevant external or off-chain data by means of queries typically through crypto-asset exchange application programming interfaces and which provides inputs to smart contracts.
Private key	A private key is a large, randomly generated string of alphanumeric characters with hundreds of digits. This secret number acts as a password to protect a crypto asset holder and is the key to unlocking access to the virtual vault that holds the crypto asset.
Proof of stake	A blockchain-specific consensus mechanism for validating entries into a distributed database and keeping the database secure based on validators' pledging or "staking" a certain amount of crypto-assets to have a chance to be chosen for the creation of a new block.
Proof of work	A blockchain-specific consensus mechanism for validating entries into a distributed database and keeping the database secure where potential validators compete with one another to solve cryptographic puzzles to be allowed to add transactions to the distributed ledger.
Smart contract	A crypto asset term that refers to self-executing applications that can trigger an action if some pre-specified conditions are met.
Stablecoin	A crypto asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.
Sybil attack	When a single entity attempts to gain control over a blockchain network using multiple fraudulent nodes.
Tokenisation	The process of creating a digital representation (token) of an asset and putting it on a distributed ledger. The information stored in tokenised form can include asset type, ownership details, valuation, legal framework, optionality, and settlement requirements, among other elements that enable significant customisation opportunities for issuer and owner to elect.
Total value locked	Industry-reported measure of the total value of assets deposited
Trustless system	A trustless system is designed to operate without relying on trust in people or institutions. It's a self-sufficient, autonomous system that can verify transactions and make sure everything is legitimate, all without any need for human intervention.

Financial Sector
Conduct Authority

Financial Sector Conduct Authority
Riverwalk Office Park, Block B, 41 Matroosberg Road, Ashlea Gardens, Pretoria, 0002
012 428 8000
www.fsca.co.za