Managing Risk in DeFi

Position Paper

Johannes Rude Jensen[1,2] Omri Ross[1,2]

[1] Department of Computer Science, University of Copenhagen
[2] eToroX Labs

j.jensen@di.ku.dk, Omri@di.ku.dk

Abstract.

Decentralized financial application (DeFi) are a new type of consumer-facing financial application composed of as 'smart contracts' deployed on a permissionless blockchain. We situate the DeFi concept in the theoretical context of permissionless blockchain and provide a taxonomical overview of agents, incentives and risks in DeFi applications. We identify four key risks with relevance for managers, practitioners and scholars contemplating a proactive engagement with decentralized financial applications. We contribute new foundational insights into a rapidly emerging field with far-reaching implications for consumer finance.

Keywords: DeFi, Blockchain Smart Contracts, Decentralized Finance.

1 Introduction

The concept of 'decentralized finance', colloquially referred to as 'DeFi', is a new breed of open financial applications deployed on permissionless blockchain infrastructure. A rapid surge in the popularity of these applications saw the total value of the assets locked in DeFi applications (TVL) grow from a range of $400-500m at the outset of 2020 to no less than $9.6bn towards the end of the third quarter of the same year[1]. While scholars within the information systems and the management disciplines recognize the novelty and prospective impact of blockchain technology, theoretical or empirical work on DeFi remains scarce [1]. In this brief position paper, we provide a conceptual introduction to 'DeFi' situated in the theoretical context of permissionless blockchain technology. We introduce a taxonomy of agents, roles, incentives and risks in DeFi applications and present four key sources of complexity and risk for managers, scholars or practitioners engaging with this new breed of financial applications.

[1] https://defipulse.com/

2 Permissionless Blockchain Technology and Decentralized Financial Applications

The novel design principles for the group of distributed database architectures referred to as 'permissionless blockchains' has generated a growing body of literature in the information systems (IS) and the management genres [2]. Primarily informed by the commercial implications of smart contract technology, scholars have examined the implications for activities in the financial services such as the settlement and clearing of 'tokenized' assets [3] the execution and compilation of financial contracts [4]–[6], complexities in supply-chain logistics [7] and beyond.

A permissionless blockchain is a type of distributed database architecture in which a decentralized network of stakeholders maintains a singleton state machine. Transactions in the database represent state transitions disseminated amongst network participants in blocks of data, typically through a standardized 'gossip' protocol. The correct order of the blocks containing the chronological overview of transactions in the database is maintained with the use of cryptographical primitives, by which all stakeholders can manually verify the succession of blocks. A network consensus protocol defines the rules for what constitutes a legitimate transaction in the distributed database. In most cases, consensus protocols are rigorous game-theoretical mechanisms in which network participants are economically incentivized to promote network security through rewards and penalties for benevolent or malicious behavior.

More recent implementations of the technology introduce a virtual machine, the state of which is maintained by the nodes supporting the network. The virtual machine is a simple stack-based architecture, in which network participants can execute metered computations denominated in the native currency format. Computational expenditures are priced on the open market, a design choice intended to mitigate excessive use of resources leading to network congestion or abuse. Network participants mostly pass instructions to the virtual machine a higher-level programming language, the later generations of which now facilitate complex programs, referred to as smart contracts. Because operations in the virtual machine are executed in a shared state, smart contracts are stateful, meaning that any applications deployed as a smart contract enjoys a high level of certainty: Once a smart contract is deployed it will execute exactly as written, a property which subsequently inspired the moniker 'the world computer'.

2.1 DeFi Applications

For the purpose of identifying risks, it is sufficient to denote the concept: 'DeFi application' as an arrangement of consumer-facing smart contracts, executing a predefined business logic within a deterministic computational environment afforded by a permissionless blockchain. DeFi applications often seek to imitate traditional financial services while removing dependencies on intermediaries. Since DeFi applications are deployed as smart contracts and thus execute a given business logic deterministically, users interact directly with the application independent of any external service providers. Contemporary DeFi applications provide a range of financial services replicating

the relative exposure or protection to certain financial events required by traders, investors or clients in the financial services. In Table 1, we present a selection of DeFi applications sorted by sector.

	Asset Management	Derivatives	Asset Exchange	Lending	Insurance
Applications	*InstaDApp; yearn.finance; Set Protocol; Melon*	*dYdX; Synthetix; Augur;*	*UniSwap; Curve Finance; Balancer; Bancor; Kyber;*	*Maker; Aave; Compound; Dharma; bZx;*	*Nexus Mutual; Opyn*

Table 1: Selected DeFi Applications by Sector

2.2 Nascent Design Principles for Decentralized Financial Applications

The metered pricing of computational resources on permissionless blockchains imposes a requirement for strict resource efficiency in the design of business logic for DeFi applications. Application designers seek to mitigate the need for expensive operations such as storing data in persistent memory or conducting sophisticated calculations in the effort of reducing the level of complexity required to execute a given service. Because the resources required for interacting with a smart contract is typically funded by the user submitting a transaction, application designers employ a combination of algorithmic financial engineering and sophisticated incentive schemes to retain liquidity and return to an equilibrium state in changing demand-scenarios. Adding to the implicit constraints of computing business logic on in a permissionless blockchain architecture, application designers face demands for a transparent and 'decentralized' governance processes from the community of stakeholders supporting the application.

Owing to the original open-source ethos of blockchain technology, the somewhat abstract and arbitrary term 'decentralization' is often posed as a strong product requirement for application designers. Often, the intention is to mitigate malicious intent such as theft of user's assets while including the community in decision-making processes and the potential profits ensuing from the growth of the application. Reacting to these demands, the tendency for issuance and distribution of so-called governance tokens; fungible units allocating voting power in a majority voting-scheme, has emerged. Like traditional equities, governance tokens trade on secondary markets and thus introduce the opportunity for capital formation for early community members of application designers. By distributing governance tokens, application designers seek to disseminate value to community members while retaining enough capital to scale development of the application by selling inventory over multiple years. With the growing market for DeFi applications, a standard terminology denoting agents and roles in DeFi applications has emerged. In table 2, we introduce a taxonomy for agents and their roles in contemporary DeFi applications, highlighting key risks associated with each role.

Agent:	Role:	Incentives for participation:	Key risk:
Users	Utilizing the application.	Profits, credit, exposure and governance token yield	Market risks, network congestion,
Liquidity Providers	Supply capital to the application in order to ensure liquidity for traders, borrowers or	Protocol fees, governance token yield	Systemic risk, admin-keys, Impermanent loss,
Arbitrageurs	Return the application to an equilibrium state through strategic purchasing and selling of assets.	Arbitrage profits	Market risk, network congestion
Application Designers (Team and Founders)	Design, implement and maintain the application	Governance token appreciation	Software bugs

Table 2: Agent classification, incentives and key risks

3 Identifying and Managing Risk in Decentralized Finance

As evident, the concept of decentralized financial applications denotes a complex and volatile environment, in which the identification of risk is instrumental. In this section, we identify and evaluate four key risk factors introducing new levels of complexity for managers, practitioners and scholars.

3.1 Software integrity and security

Owing to the deterministic nature of permissionless blockchain technology, applications deployed on as smart contracts are subject to excessive security risks, as any signed transaction remains permanent once included in a block. The irreversible or, 'immutable' nature of transactions in a blockchain network has led to significant loss of capital on multiple occasions, most frequently as a result of errors in the code, sometimes relating to even the most sophisticated aspects virtual machine semantics [8].

3.2 Transaction costs, protocol fees and network congestion

To mitigate abusive or excessive use of the computational resources available on the network, computational resources required to interact with smart contracts are metered in the native asset class. This creates a secondary market for transactions, in which users

outbid each other by attaching transaction fees in the effort of incentivizing miners to select their transaction for inclusion in the next block. In times of network congestion, transaction fees appreciate to an extent to which single applications or sub-components gross several hundreds of thousands of dollars from users seeking to interact with the application.[2] While intermediary service providers occasionally choose to subsidize protocol transaction fees[3], application fees are in near all cases paid by the user signing a transaction. Because application designers seek to lower the aggregate transaction costs, protocol fees, slippage or impermanent loss through algorithmic financial modelling and incentive alignment, managers, practitioners and scholars ought to observe the state of the network and the application with which they are interacting, diligently. If a period of network congestion coincides with a period of volatility pushing an application out of a programmed equilibrium, the application design may impose excessive application fees or penalties on otherwise standard actions such as withdrawing or adding liquidity.

3.3 Participation in decentralized governance

Responding to implications of the historically concentrated distribution of native assets amongst a small minority of stakeholders, DeFi application designers increasingly rely on a gradual distribution of fungible governance-tokens in the attempt at adequately 'decentralizing' decision-making processes. While the distribution of governance tokens remains fairly concentrated amongst a small group of colluding stakeholders, the gradual distribution of voting-power to liquidity providers and users will result in an increasingly long-tailed distribution of governance tokens. Managers, practitioners and scholars ought to observe the decision-making process, familiarizing themselves with the governance logic of the platform and potentially adversarial implications of a given set of governance outcomes.

3.4 Interoperability and systemic risk

A key value proposition for DeFi applications is the level of interoperability enjoyed by end-users, often referring to the set of applications colloquially as 'money Legos'. As most applications are deployed on the Ethereum blockchain, users can transact seamlessly between different applications with settlement times rarely exceeding a few minutes, a factor which facilitates rapid capital flows between old and new applications on the network. While interoperability is an attractive feature for any set of financial applications, tightly coupled and complex liquidity systems can generate an excessive degree of financial integration, resulting in systemic dependency between applications [9]. This factor is exacerbated by the often complex and heterogeneous methodologies for computation of exposure, debt, value and collateral value in DeFi applications. The ensuing degree of contagion may introduce systemic risks, as a sudden failure or exploit in one application will ripple throughout the network, affecting stakeholders across the

[2] https://etherscan.io/gastracker
[3] Coinbase.com

entire ecosystem of applications. Managers, practitioners and scholars engaging with these applications financially ought to observe the entire field of applications with macro-prudential rigor.

4 Conclusion: Is DeFi The Future of Finance?

DeFi introduces novel complexities and risks with relevance for both scholars and practitioners, engaging with this new class of financial application. In this position paper, we examine potential implications, complexities and risks associated with the proliferation of consumer-facing DeFi applications within the financial services. We provide a taxonomical overview of DeFi applications and identify four key risks for managers, practitioners and scholars contemplating a proactive engagement with decentralized financial applications.

5 References

[1] J. Kolb, M. Abdelbaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain: A centralized tutorial," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–39, 2020.

[2] O. Labazova, "Towards a Framework for Evaluation of Blockchain Implementations," in *Fortieth International Conference on Information Systems*, 2019.

[3] O. Ross, J. Jensen, and T. Asheim, "Assets under Tokenization: Can Blockchain Technology Improve Post-Trade Processing?," in *Fortieth International Conference on Information Systems, Munich 2019*, 2019.

[4] J. R. Jensen and O. Ross, "Settlement with Distributed Ledger Technology," in *Forty-First International Conference on Information Systems*, 2020.

[5] B. Egelund-Müller, M. Elsman, F. Henglein, and O. Ross, "Automated Execution of Financial Contracts on Blockchains," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 457–467, 2017.

[6] O. Ross and J. R. Jensen, "Compact Multiparty Verification of Simple Computations," in *BIR Workshops*, 2018.

[7] B. Düdder and O. Ross, "Timber tracking: reducing complexity of due diligence by using blockchain technology (position paper)," in *2nd Workshop on Managed Complexity*, 2017.

[8] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making Smart Contracts Smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 2016,

[9] L. Gudgeon, D. Perez, D. Harz, B. Livshits, and A. Gervais, "The Decentralized Financial Crisis," pp. 1–15, 2020.