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 applications (DeFi) are a new breed of consumer-facing financial applications composed as smart contracts, deployed on permissionless blockchain technologies. We situate the DeFi concept in the theoretical context of permissionless blockchain technology and provide a taxonomical overview of agents, incentives and risks in DeFi applications. We identify four key risk groups for potential stakeholders contemplating the advantages of decentralized financial applications. We contribute novel insights into a rapidly emerging field, with far-reaching implications for the financial services.

Keywords: DeFi, Blockchain Smart Contracts, Decentralized Finance.

1 Introduction

Decentralized financial applications, colloquially referred to as 'DeFi', is a new type of open financial applications deployed on openly accessible, permissionless blockchains. 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 management disciplines recognize the novelty and prospective impact of blockchain technologies, 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 potential sources of complexity and risk.

[1] https://defipulse.com/

2 Permissionless Blockchain Technology and Decentralized Financial Applications

The implications and design principles for blockchain and distributed ledger technologies have 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 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. 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 [8]. Scholars typically differentiate between 'permissioned' and 'permissionless' blockchains. Permissionless blockchains are open environments accessible by all, whereas permissioned blockchains are inaccessible for external parties not recognized by a system administrator [2].

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. Because all 'nodes' running the blockchain 'client' software must replicate the computations required for a program to run, computational expenditures are priced on the open market. This design choice is intended to mitigate excessive use of resources leading to network congestion or abuse. Network participants pass instructions to the virtual machine in a higher-level programming language, the most recent generations of which is used to write programs, referred to as *smart contracts*. Because operations in the virtual machine are executed in a shared state, smart contracts are both transparent and *stateful*, meaning that any application deployed as a smart contract executes deterministically. This means that once a smart contract is deployed, it will execute exactly as instructed.

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 the transparent and deterministic computational environment afforded by a given permissionless blockchain. 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 within asset management, derivatives, lending, and insurance services.

The metered pricing of computational resources on permissionless blockchains means that DeFi applications are constrained by the computational resources they can use. Application designers seek to mitigate the need for the most expensive operations, such as storing big amounts of data or conducting sophisticated calculations, in the effort of reducing the level of complexity required to execute the service that their application provides.

Because the resources required for interacting with a smart contract is paid by the user, DeFi application designers employ an innovative combination of algorithmic financial engineering and game theory to ensure that all stakeholders of their application are sufficiently compensated and incentivized. In table 2, we introduce a taxonomy for the different types of agents and their roles in contemporary DeFi applications. We highlight the incentives for participation and 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

Owing to the original open-source ethos of blockchain technology, application designers are required to be transparent and build ‘open’ and accessible applications, in which users can take ownership and participate in decision-making processes, primarily concerning new features or changes to the applications. As a reaction to these demands, application designers often issue and distribute so-called *governance tokens*.

Governance tokens are fungible units held by users, which allocates voting power in majority voting-schemes. Much like traditional equities, governance tokens trade on secondary markets which introduces the opportunity for capital formation for early stakeholders and designers of successful applications. 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.

3 Identifying and Managing Risk in Decentralized Finance

Decentralized financial applications introduce a complex and volatile environment. In this section, we identify and evaluate the four key risk factors which may introduce complexities for stakeholders involved with these applications.

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 coding errors, sometimes relating to even the most sophisticated aspects virtual machine and programming language semantics [9].

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. This creates a secondary market for transactions, in which users can 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 interacting 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 interacting with the DeFi application. Because application designers seek to lower the aggregate transaction costs, protocol fees, slippage or impermanent loss through algorithmic financial modelling and incentive alignment, stakeholders must carefully observe the state of the blockchain network. If a period of network congestion coincides with a period of volatility, the application design may suddenly impose excessive fees or penalties on otherwise standard actions such as withdrawing or adding funds to a lending market.

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

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. Broad distributions of governance tokens may result in adversarial implications of a given set of governance outcomes, for stakeholders who are not sufficiently involved in monitoring the governance process.

3.4 Application interoperability and systemic risks

A key value proposition for DeFi applications is the level of interoperability between applications. As most applications are deployed on the Ethereum blockchain, users can transact seamlessly between different applications with settlement times rarely exceeding a few minutes. This 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 [10]. This factor is exacerbated by the often complex and heterogeneous methodologies for the computation of exposure, debt, value, and collateral value that DeFi application designers have used to improve their product. An increasing degree of contagion between application may introduce systemic risks, as a sudden failure or exploit in one application could ripple throughout the network, affecting stakeholders across the entire ecosystem of applications.

4 Conclusion: Is DeFi The Future of Finance?

In this position paper, we have examined the potential implications, complexities and risks associated with the proliferation of consumer facing DeFi applications. While DeFi applications deployed on permissionless blockchains present a radical potential for transforming consumer facing financial services, the risks associated engaging with these applications remain salient. Practitioners contemplating an engagement with these applications ought to consider and evaluate key risks prior to committing or allocating funds to DeFi applications. Scholars interested in DeFi applications may approach the theme from numerous angles, extending early research on the market design of DeFi applications [11] or issues related to governance tokens [12] and beyond.

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] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and Dapps*. O'Reilly Media, 2018.

[9] 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, vol. 24-28-Octo, pp. 254–269.

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

[11] G. Angeris, H.-T. Kao, R. Chiang, C. Noyes, and T. Chitra, "An analysis of Uniswap markets," pp. 1–25, 2019.

[12] G. Tsoukalas and B. H. Falk, "Token-Weighted Crowdsourcing Token-Weighted Crowdsourcing," *Manag. Sci. 66(9)3843-3859. https// doi.org/10.1287/mnsc.2019.3515 Full*, no. October, 2020.