Towards a Theory of Decentralized Finance

Massimo Bartoletti[1], James Hsin-yu Chiang[2], Alberto Lluch Lafuente[2]

[1] Università degli Studi di Cagliari, Cagliari, Italy
[2] Technical University of Denmark, DTU Compute, Copenhagen, Denmark

Abstract. Decentralized Finance (DeFi) has brought about decentralized applications which allow untrusted users to lend, borrow and exchange crypto-assets. Many of such applications fulfill the role of markets or market makers, featuring complex, highly parametric incentive mechanisms to equilibrate interest rates and prices. This complexity makes the behaviour of DeFi applications difficult to understand: indeed, ill-designed incentive mechanisms could potentially lead to emergent unwanted behaviours. We argue that theories, techniques and tools rooted in formal methods can provide useful instruments to better understand, specify and analyze DeFi systems. We summarize in this paper our first steps towards a theory of DeFi based on formal methods, and we overview the open challenges and opportunities for formal methods in DeFi.

1 DeFi Archetypes and their Formalization

The emergence of permissionless, public blockchains has given birth to an entire ecosystem of *crypto-tokens* representing digital assets and derivatives. Facilitated and accelerated by smart contracts and standardized token interfaces [1], these so-called *decentralized finance* (DeFi) applications promise an open alternative to the traditional financial system. Prior foundational research in the domain of DeFi has been thoroughly summarized in [24].

To study properties emerging from the interaction between users and DeFi applications, we have initiated our line of research towards a theory of DeFi by focusing on the identification of *archetypal* DeFi applications and on the development of *executable specifications* for them, based on manual inspection of the underlying implementations of mainstream implementations. Our formal specifications encompass (abstractions of) the underlying economic incentive mechanisms [5, 15, 16] and pave the way towards a generalized theory of DeFi archetypes and their interactions, which may be intractable from analysis at the implementation level alone. These executable semantics represents a first step towards *domain-specific languages* for decentralized finance, where DeFi contracts are composed from formally specified primitives and thus exhibit well-defined, analyzable behaviour inferred from the language semantics. The main archetypes we have considered so far are *Lending Pools* (LPs) [7] and *Automatic Market Makers* (AMMs) [8].

Lending Pools Lending pools are decentralized applications which allow mutually untrusted users to lend and borrow crypto-assets. In [7], we formalize all interactions between users and LPs, thereby providing a complete specification for the economic functionality of LPs. Our model allows to formally state and specify fundamental properties of LPs, like e.g. correct accounting of *minted* tokens and preservation of the supply of *deposited* tokens, which are crucial to ensure consistency in exchange and distribution of tokens enabled by LPs. Furthermore, our model allows one to reason about rational agents, which are incentivized to liquidate loans in return for discounted collateral or perform deposits immediately prior to interest accrual. We also provide solid arguments for the design of incentives of LPs, for example by formally proving that depositors can potentially redeem more tokens than they deposited, and by identifying the conditions under which redeems are not possible. In this regard, we formalize notions of *utilization safety,* which represents a utility trade-off between borrow and redeem actions, moderated by a dynamic interest rate. In LPs, loans are secured by collateral: yet, there exist LP states in which the borrower is no longer incentivized to return loan should the agent's collateralization drop below a certain threshold. We formally characterize such *collateral-safe* states. Finally, we exploit both notions of safety to illustrate attacks on utilization and collateralization, aimed at undermining the incentive mechanisms of LPs.

Automatic Market Makers Automatic market makers allow users to exchange units of different types of crypto-assets, without the need to find a counter-party. In [8], we develop a theory for AMMs, specifying their possible interactions and their economic mechanisms. One of the results we provide is a concurrency theory for AMM actions. In particular, we show that sequences of *deposit* and *redeem* actions can be ordered interchangeably, resulting in observationally equivalent AMM states. We prove fundamental preservation properties for our AMM specification, like e.g. the preservation of deposited token supplies, and *token liquidity*, which ensures that deposited tokens cannot be *frozen* in an AMM application. Furthermore, we introduce a formal notion of *incentive-consistency*: AMM's rely on a dynamic exchange rate governed by a so-called *trading invariant*. Notably, we formalize the key incentive mechanism, the arbitrage game, for all trading invariants which are *incentive-consistent*, thus facilitating formal analysis of AMM behaviour which can be generalized beyond the mainstream constant-product AMMs.

2 Next Steps, Challenges and Opportunities

The identification and formalization of DeFi archetypes is only the first step towards a general theory of DeFi. There are many steps ahead, and new avenues for future research, full of challenges and opportunities. We discuss some of them, focusing mostly on issues that arise when considering DeFi ecosystems as composed by a set of collaboration or competing agents, interacting through possibly separate contract execution environments enabled by miners, who may have transaction ordering privileges and their own goals.

Agent strategies The formal methods toolbox provides a plethora of specification tools and languages to specify systems composed of concurrent actors [21, 25]. In order to formally analyze the emergent behaviour of such a system, a specification of all user strategies must be defined or synthesised. Here we distinguish between *rational* strategies, which are risk-free actions increasing the user's net wealth and strategies which are *speculative*, driven by an agent's *expectation* of a future system state which is not guaranteed: attempting a liquidation action, for example, is a rational strategy as the actor will obtain collateral at a discounted rate or at worst, fail to execute any action at all if the transaction fails. On the other hand, depositing funds in a LP is speculative, as it is based on an expectation of future interest, regulated by future actions of borrowers and depositors.

Whereas there appears to be a clear path towards formal specification of rational strategies in DeFi systems, the specification of speculative agent behaviour in DeFi remains an open question. For individual DeFi archetypes, agent-based models have been proposed [2, 17] with a focus on rational behaviour, yet the specification of economically speculative strategies in a wider, composition of DeFi application remains an open research challenge.

Classical agent-based models from economic disciplines feature specification techniques of economically (speculative) agent behaviour: here, we also observe that stochastic model checking tools from formal methods are increasingly deployed [22] in the economic research community and suggest that stochastic model checking of agent-based models of DeFi systems may provide a path forward towards the automatic analysis of agent strategies.

A model of transaction concurrency Actions performed in DeFi systems are generally not concurrent: this is observable with AMMs, for example, where an actor with transaction ordering privileges can benefit from ordering its own transaction before and after that of the victim [18,26]. More generally, the ability of miners to extract value beyond transaction fees from specific sequences of DeFi interactions has been denoted miner-extractable-value (MEV) [13]. Thus, a formal model of a DeFi system composed by different DeFi applications must also feature a notion of *incentive-consistent* action sequences in the presence of rational agents with transaction ordering privileges.

Such analysis is further complicated by atomic chains of transactions, such as those obtained by nested contract calls in Ethereum. Here, the sequencing of individual actions within the call-chain is determined by the authorizing user: this can result in DeFi exploits amplified by flash loans [10, 19, 23]. As transactions, call-chains must also exhibit consistency with miner transaction ordering incentives: here, we note a lack of formal models to integrate call-chain semantics with formal models of MEV.

A model of transaction ordering may ultimately facilitate the automated analysis of a DeFi system specification, given that it narrows the set of *valid* interaction sequences. Given sufficiently specified agent strategies, such a theory may pave the way towards novel model checking techniques in DeFi.

Cryptographic protocol composition Cryptographic protocols play an increasingly central role in DeFi systems, as they allow DeFi applications to keep private selected parts of the application state: public execution introduces incentives (MEV) which challenge DeFi security, but the public execution of user actions also compromises privacy. The popularity of crypto-asset mixers [4] powered by ZK-SNARK proofs on the Ethereum blockchain foreshadows the emergence of privacy-focused DeFi applications, which in turn, may open new approaches to mitigate MEV. Private order-matching has been proposed with multi-party-computation techniques [11], and we foresee similar techniques for DeFi applications. Furthermore, advanced cryptographic protocols improve scalability: many DeFi applications have migrated to ZK-rollups [3] in order to absorb the increased user demand on the Ethereum blockchain.

For the secure composition of cryptographic protocols deployed for both privacy and scalability, the formal methods community may contribute both classical information flow [12] analysis techniques and cryptographic protocol composition analysis [14]: as a multitude of privacy-focused and scalable applications are composed in a single system, we highlight the formal analysis of safe cryptographic protocol composition in DeFi as an new research frontier.

Domain-specific languages Since the analysis of security aspects of DeFi applications will invariably involve specifications of agents and miners, higher abstractions of DeFi specification will arguably be of interest to the DeFi and formal methods communities. Domain-specific languages with formal semantics (e.g. [6, 9, 20]) provide suitable specification means for such abstractions. Moreover, they fulfill two purposes: firstly, they enable formal reasoning and security proofs. Secondly, DeFi-specific languages can provide built-in security guarantees, given a foundational theory of the underlying DeFi system.

3 Concluding Remarks

We thank the organizing committee of the first edition of the DeFi workshop for the fruitful exchange of research ideas on the topic of decentralized finance and encourage the DeFi community to join us in extending the formal methods toolkit in addressing the open security challenges in decentralized finance present today and those emerging on the horizon.

Acknowledgements The second author is supported by the PhD School of DTU Compute. The third author is partially supported by the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu).

References

1. ERC-20 token standard (2015), https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md
2. Uniswap oracle template (2020), https://github.com/Uniswap/uniswap-v2-periphery/blob/dda62473e2da448bc9cb8f4514dadda4aeede5f4/contracts/examples/ExampleOracleSimple.sol
3. Starkware (2021), https://starkware.co/
4. Tornado (2021), https://tornado.cash/
5. Angeris, G., Evans, A., Chitra, T.: When does the tail wag the dog? Curvature and market making. arXiv preprint arXiv:2012.08040 (2020), https://arxiv.org/pdf/2012.08040
6. Arusoaie, A.: Certifying Findel derivatives for blockchain. Journal of Logical and Algebraic Methods in Programming **121**, 100665 (2021). https://doi.org/https://doi.org/10.1016/j.jlamp.2021.100665
7. Bartoletti, M., Chiang, J.H., Lluch-Lafuente, A.: SoK: Lending pools in decentralized finance. In: 5th Workshop on Trusted Smart Contracts (2021), (to appear) https://arxiv.org/abs/2012.13230
8. Bartoletti, M., Chiang, J.H., Lluch-Lafuente, A.: A theory of automated market makers in defi. arXiv preprint arXiv:2102.11350 (2021), http://arxiv.org/abs/2102.11350
9. Bartoletti, M., Zunino, R.: BitML: a calculus for Bitcoin smart contracts. In: ACM CCS (2018). https://doi.org/10.1145/3243734.3243795
10. Cao, Yixin and Zou, Chuanwei and Cheng, Xianfeng: Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem. arXiv preprint arXiv:2102.00626 (2021), https://arxiv.org/pdf/2102.00626
11. Carsten Baum and Bernardo David and Tore Frederiksen: P2DEX: Privacy-Preserving Decentralized Cryptocurrency Exchange. Cryptology ePrint Archive, Report 2021/283 (2021), https://eprint.iacr.org/2021/283
12. Cecchetti, Ethan and Yao, Siqiu and Ni, Haobin and Myers, Andrew C: Compositional Security for Reentrant Applications. arXiv preprint arXiv:2103.08577 (2021), http://arxiv.org/abs/2103.08577
13. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.: Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In: IEEE Symposium on Security and Privacy. pp. 910–927. IEEE (2020). https://doi.org/10.1109/SP40000.2020.00040
14. Dolev, Danny and Yao, Andrew: On the security of public key protocols. IEEE Transactions on information theory **29**(2), 198–208 (1983)
15. Evans, A., Angeris, G., Chitra, T.: Optimal Fees for Geometric Mean Market Makers (2021), https://web.stanford.edu/~guillean/papers/g3m-optimal-fee.pdf
16. Gudgeon, L., Werner, S., Perez, D., Knottenbelt, W.J.: Defi protocols for loanable funds: Interest rates, liquidity and market efficiency. In: ACM Conference on Advances in Financial Technologies. pp. 92–112 (2020). https://doi.org/10.1145/3419614.3423254
17. Kao, H.T., Chitra, T., Chiang, R., Morrow, J.: An Analysis of the Market Risk to Participants in the Compound Protocol https://scfab.github.io/2020/FAB2020_p5.pdf
18. Qin, K., Zhou, L., Gervais, A.: Quantifying blockchain extractable value: How dark is the forest? (2021), https://arxiv.org/pdf/2101.05511

19. Qin, K., Zhou, L., Livshits, B., Gervais: Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. In: Financial Cryptography (2021), (to appear) https://arxiv.org/pdf/2003.03810
20. Seijas, P.L., Thompson, S.J.: Marlowe: Financial contracts on blockchain. In: ISoLA. LNCS, vol. 11247, pp. 356–375. Springer (2018). https://doi.org/10.1007/978-3-030-03427-6_27
21. Tolmach, P., Li, Y., Lin, S.W., Liu, Y.: Formal Analysis of Composable DeFi Protocols. In: 1st Workshop on Decentralized Finance (2021), (to appear) https://arxiv.org/abs/2103.00540
22. Vandin, Andrea and Giachini, Daniele and Lamperti, Francesco and Chiaromonte, Francesca: Automated and Distributed Statistical Analysis of Economic Agent-Based Models. arXiv preprint arXiv:2102.05405 (2021)
23. Wang, Dabao and Wu, Siwei and Lin, Ziling and Wu, Lei and Yuan, Xingliang and Zhou, Yajin and Wang, Haoyu and Ren, Kui: Towards understanding flash loan and its applications in defi ecosystem. arXiv preprint arXiv:2010.12252 (2020), https://arxiv.org/pdf/2010.12252
24. Werner, S.M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.J.: Sok: Decentralized finance (DeFi) (2021)
25. Zhao, Wenqi and Li, Hui and Yuan, Yuming: (2021), (to appear) https://arxiv.org/abs/2101.08423
26. Zhou, L., Qin, K., Torres, C.F., Le, D.V., Gervais, A.: High-Frequency Trading on Decentralized On-Chain Exchanges. arXiv preprint arXiv:2009.14021 (2020), https://arxiv.org/pdf/2009.14021