Report from Dagstuhl Seminar 22421

Security of Decentralized Financial Technologies

Arthur Gervais[*1], **and Marie Vasek**[*2]

1 **Imperial College London, GB.** arthur@gervais.cc
2 **University College London, GB.** m.vasek@ucl.ac.uk

Abstract

The decentralized finance (DeFi) sector has grown to a 13+ billion USD economy, encompassing various financial activities. The non-custodial nature of DeFi requires users to take responsibility for managing their assets, but it also provides them more control over their assets. The Dagstuhl Seminar brought researchers together to examine the security, privacy, and financial properties of DeFi and explore ways to protect users. The seminar aimed to reconcile the conflicting demands of security, usability, and performance in DeFi and outline best practices. Despite progress made in the DeFi sector, there is still much to be explored and improved, such as user education, regulatory compliance, and the scalability and performance limitations of decentralized ledgers. To build a secure and user-friendly DeFi ecosystem, continued collaboration among experts is needed.

Seminar October 16–21, 2022 – http://www.dagstuhl.de/22421
2012 ACM Subject Classification Information systems → Digital cash; Security and privacy → Cryptography; Security and privacy → Distributed systems security
Keywords and phrases blockchain technology, decentralized finance (DeFi), distributed consensus protocols, security economics, security foundations
Digital Object Identifier 10.4230/DagRep.12.10.129

1 Summary

Arthur Gervais
Marie Vasek

Trusted intermediaries have been the backbone of economic transactions for centuries. However, with the rise of decentralized ledgers like Bitcoin and Ethereum, individuals now have the opportunity to trade and interact without relying on a centralized authority. In 2020, the decentralized finance (DeFi) sector grew to become a 13+ billion USD economy, encompassing exchanges, borrowing/lending, margin trading, derivatives, and more.

The non-custodial nature of decentralized ledgers gives individuals more control over their assets, but it also requires them to take greater responsibility for managing their private keys and assets. Cryptographers expect DeFi users to have a deep understanding of the security properties and guarantees of the protocols, but in reality, it is challenging to keep users informed about these complexities. Therefore, there is a pressing need for more research to clarify user comprehension of DeFi properties. Additionally, decentralized ledgers face a number of technical limitations, such as scalability issues and potential vulnerabilities to pseudonymous malicious actors.

[*] Editor / Organizer

Security of Decentralized Financial Technologies, *Dagstuhl Reports*, Vol. 12, Issue 10, pp. 129–142
Editors: Arthur Gervais and Marie Vasek
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

To address these challenges, the Dagstuhl Seminar brought together researchers with expertise in various subfields of DeFi to jointly examine the security, privacy, and financial properties of decentralized finance. The primary objective of the seminar was to explore how to protect DeFi users. The seminar aimed to reconcile the conflicting demands of security, usability, and performance in DeFi, and outline best practices for users to remain safe while engaging in DeFi activities. Finally, the seminar aimed to apply its recommendations to the growing DeFi ecosystem.

During the seminar, participants presented talks on a wide range of topics, including active attacks on the DeFi ecosystem, proposed cryptographic schemes for enhancing the security of cryptocurrencies, and network insights on cryptocurrencies. The seminar also featured productive discussions across working groups, bringing together researchers from diverse perspectives to achieve the common goal of securing the DeFi landscape.

Given the rapid growth of the DeFi sector, it is important to keep exploring ways to improve its security and user-friendliness. One way to do this is through collaboration and information-sharing among researchers, developers, and users. The Dagstuhl Seminar was an important step in this direction, but there is still much work to be done.

One area of focus could be on improving user education and awareness. This could include developing easy-to-understand guides and tutorials, as well as increasing the transparency of DeFi protocols and the risks associated with using them. Additionally, there is a need for more research into the scalability and performance limitations of decentralized ledgers, as well as finding ways to mitigate security risks such as smart contract vulnerabilities.

Another important aspect to consider is the regulatory landscape for DeFi. Currently, many DeFi protocols operate in a regulatory gray area, and it is important to ensure that they comply with relevant laws and regulations while also protecting user privacy and security. This may require more collaboration between DeFi developers and regulators to establish clear guidelines and standards.

Despite the progress made in the DeFi sector, there are still many unknowns that need to be explored. For example, there is limited understanding of how the Ethereum Proof-of-Stake (PoS) security mechanism works, and what guarantees it provides. This is a crucial aspect of the DeFi landscape as Ethereum is the most widely used blockchain for DeFi applications. Further research is needed to understand the security properties of Ethereum PoS and how it can be improved to better protect users. Additionally, there are other areas in DeFi that require further investigation, such as the scalability and performance limitations of decentralized ledgers, and the trade-offs between privacy and security. By exploring these unknowns, we can gain a better understanding of the DeFi ecosystem and find ways to improve its security and user-friendliness.

In conclusion, the DeFi sector is still in its early stages, and there is much room for growth and improvement. By continuing to bring together experts from various fields and encouraging collaboration, we can help to build a secure and user-friendly DeFi ecosystem that benefits everyone.

2 Table of Contents

Summary

Overview of Talks

Working groups

3 Overview of Talks

3.1 Concrete bounds for PoW

Rainer Böhme (Universität Innsbruck, AT)

Joint work of Rainer Böhme, Patrik Keller
Main reference Patrik Keller, Rainer Böhme: "Parallel Proof-of-Work with Concrete Bounds", CoRR, Vol. abs/2204.00034, 2022.
URL https://doi.org/10.48550/arXiv.2204.00034

We review the succession of work leading to concrete bounds for the failure probability of Bitcoin's proof-of-work mechanism in adversarial synchronous networks. While Bitcoin uses proof-of-work sequentially, we propose to study concrete bounds for state replication protocols using non-sequential proof-of-work. Numerical analyses suggest that after the typical interval of 10 minutes, a novel parallel proof-of-work protocols offers two orders of magnitude more security than sequential proof-of-work. This means that state updates could be sufficiently secure to support commits after one block (i.e., after 10 minutes), removing the risk of double-spending in many applications.

3.2 Miner Extractable Value (MEV) and Flash Freezing Flash Boys (F3B)

Bryan Ford (EPFL Lausanne, CH)

Joint work of Bryan Ford, Haoqian Zhang, Louis-Henri Merino, Vero Estrada-Galiñanes

Front-running attacks, which benefit from advanced knowledge of pending transactions, have proliferated in the blockchain space since the emergence of decentralized finance. Front-running causes devastating losses to honest participants and continues to endanger the fairness of the ecosystem. We present Flash Freezing Flash Boys (F3B), a blockchain architecture that addresses front-running attacks using threshold cryptography. In F3B, a user generates a symmetric key to encrypt their transaction, and once the underlying consensus layer has committed the transaction, a decentralized secret-management committee reveals this key. F3B mitigates front-running attacks because an adversary can no longer read the content of a transaction before commitment, thus preventing the adversary from benefiting from advanced knowledge of pending transactions. Unlike other threshold-based approaches where the user encrypts their transaction based on the key of a future block, F3B enables the user to generate their key for each transaction. This feature ensures the confidentiality that all uncommitted transactions are not revealed, even if they are delayed. F3B addresses front-running at the execution layer; thus, our solution is agnostic to the underlying consensus algorithm and compatible with existing smart contracts. We evaluated F3B based on Ethereum, demonstrating a 0.05% transaction latency overhead with a secret-management committee of 128 members, indicating our solution is practical at a low cost.

3.3 What can we learn from four years of attacks on Decentralized Finance?

Arthur Gervais (Imperial College London, GB)

Within just four years, the blockchain-based Decentralized Finance (DeFi) ecosystem has accumulated a peak total value locked (TVL) of $253 billion USD. Unfortunately, this increase in DeFi's popularity has been accompanied by a number of attacks that have cost at least $3.24 billion USD between 2018 and 2022. In this talk, we offer a method for measuring, analyzing, and comparing DeFi attacks. By presenting cutting-edge defense strategies that go beyond the conventional smart contract code auditing approaches, we also hope to summarize the insights discovered to strengthen DeFi security.

3.4 Ethereum P2P Network Topology

Lucianna Kiffer (ETH Zürich, CH)

Blockchain protocols' primary security goal is consensus: one version of the global ledger that everyone in the network agrees on. Their proofs of security depend on assumptions on how well their peer-to-peer (P2P) overlay networks operate. Further, the Defi ecosystem built on top of these protocols also explicitly and inexplicably make similar assumptions.Yet, surprisingly, little is understood about what factors influence the P2P network properties. In this talk, I present work where we extensively study the Ethereum P2P network's connectivity and its block propagation mechanism. We gather data on the Ethereum network by running the official Ethereum client, geth, modified to run as a "super peer" with many neighbors. We run this client in North America for over seven months, as well as shorter runs with multiple vantages around the world. Our results expose an incredible amount of churn, and a surprisingly small number of peers who are actually useful (that is, who propagate new blocks). We also find that a node's location has a significant impact on when it hears about blocks, and that the precise behavior of this has changed over time (e.g., nodes in the US have become less likely to hear about new blocks first). Our results motivate questions on how these open systems can be manipulated and whether we should move to more structured/purposeful networks.

3.5 ROAST: Robust Asynchronous Schnorr Threshold Signatures

Tim Ruffing (Blockstream – Victoria, CA)

Joint work of Tim Ruffing, Viktoria Ronge, Elliott Jin, Jonas Schneider-Bensch, Dominique Schröder
Main reference Tim Ruffing, Viktoria Ronge, Elliott Jin, Jonas Schneider-Bensch, Dominique Schröder: "ROAST: Robust Asynchronous Schnorr Threshold Signatures", in Proc. of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022, pp. 2551–2564, ACM, 2022.
URL https://doi.org/10.1145/3548606.3560583

Bitcoin and other cryptocurrencies have recently introduced support for Schnorr signatures whose cleaner algebraic structure, as compared to ECDSA, allows for simpler and more practical constructions of highly demanded "t-of-n" threshold signatures. However, existing Schnorr threshold signature schemes still fall short of the needs of real-world applications due to their assumption that the network is synchronous and due to their lack of robustness, i.e., the guarantee that honest signers are able to obtain a valid signature even in the presence of other malicious signers who try to disrupt the protocol. This hinders the adoption of threshold signatures in the cryptocurrency ecosystem, e.g., in second-layer protocols built on top of cryptocurrencies.

In this work, we propose ROAST, a simple wrapper that turns a given threshold signature scheme into a scheme with a robust and asynchronous signing protocol, as long as the underlying signing protocol is semi-interactive (i.e., has one preprocessing round and one actual signing round), provides identifiable aborts, and is unforgeable under concurrent signing sessions. When applied to the state-of-the-art Schnorr threshold signature scheme FROST, which fulfills these requirements, we obtain a simple, efficient, and highly practical Schnorr threshold signature scheme.

3.6 State of Signatures in Bitcoin

Tim Ruffing (Blockstream – Victoria, CA)

Support for Schnorr signatures has been activated in Bitcoin in the as part of "Taproot" softfork. This talk sheds light on the motivation behind this technical change, namely a better provably security as compared to ECDSA, improved efficiency, and most importantly the possibility to construct more practical variants of advanced signature protocols such as multisignatures, threshold signature and blind signatures.

We then give an overview of the state-of-art in these areas, touching upon recent results in the area of Schnorr multisignatures signatures (e.g., MuSig2, FROST, ROAST) as well as blind signatures (e.g., Fuchsbauer, Plouviez and Seurin 2020). We also discuss open research questions in this area, e.g., how multisignatures and threshold signatures can be nested (with a tree-style key setup) while maintaining security under concurrent sessions and privacy, and whether the practicality of distributed key-generation protocols can be improved.

3.7 Suboptimality in DeFi

Aviv Yaish (The Hebrew University of Jerusalem, IL)

Joint work of Aviv Yaish, Maya Dotan, Kaihua Qin, Aviv Zohar, Arthur Gervais

The Decentralized Finance (DeFi) ecosystem has proven to be immensely popular in facilitating financial operations such as lending and exchanging assets, with Ethereum-based platforms holding a combined amount of more than 30 billion USD. The public availability of these platforms' code together with real-time data on all user interactions and platform liquidity has given rise to sophisticated automatic tools that recognize profit opportunities on behalf of users and seize them.

In this work, we formalize three core DeFi primitives which together are responsible for a daily volume of over 100 million USD in Ethereum-based platforms alone: (1) lending and borrowing funds, (2) liquidation of insolvent loans using swaps, and (3) using *flashswaps* to close arbitrage opportunities between cryptocurrency exchanges. The profit which can be made from each primitive is then cast as an optimization problem that can be solved.

We use our formalization to analyze several case studies for each primitive, showing that popular platforms and tools which promise to automatically optimize profits for users, actually fall short. In specific instances, the profits can be increased by more than 100%, with the highest amount of "missed" revenue by a single suboptimal action equal to 428.14 ETH, or roughly 517K USD.

Finally, we show that many missed opportunities to make a profit do not go unnoticed by other users. Indeed, suboptimal transactions are sometimes immediately followed by "trailing" back-running transactions which extract additional profits using similar actions. By analyzing a subset of these events, we uncover that users who frequently create such trailing transactions are heavily tied to specific miners, meaning that all of their transactions appear only in blocks mined by one miner in particular. As a portion of the backrun non-optimal transactions are private, we hypothesize that the users who create them are, in fact, miners (or users collaborating with miners) who use inside information known only to them to make a profit, thus gaining an unfair advantage.

4 Working groups

4.1 Human Aspects of DeFi and Cryptocurrencies

Svetlana Abramova (Universität Innsbruck, AT), Markus Dürmuth (Leibniz Universität Hannover, DE)

In this discussion group, we considered decentralized finance systems and cryptocurrencies from the point of view of a (human) user. We identified a number of interesting topics that can guide future research, as well as some related challenges.

Trust of users in the system seems crucial for their participation. A tentative list of factors influencing trust may include "fairness" of transaction ordering, which influences who can buy rare goods (such as NFTs). The presence of MEVs, and the fact that currently mostly powerful market players can utilize those, could be adverse for the trust; and obviously "stability" as discussed in another group. Another topic may be privacy related concerns, and the question with regards to which entities users wish privacy of financial transactions. Governance and decision making in the DeFi & cryptocurrency space is another interesting factor in itself, and may again influence trust in a system. The usability of crypto-wallets provides some very interesting use-case for user authentication, due to their pronounced requirements in availability.

We also identified a number of challenges that need to be overcome to conduct research. Recruitment of users for surveys or user studies is not easy as central methods to directly contact such users are rare, and for services claiming to sample from blockchain users it's not easy to (non-intrusively) verify those claims. This is additionally complicated by the high heterogeneity of the user-base of cryptocurrencies/DeFi (found by previous studies) and wrong mental models. In many fields, recruitment of decision makers as research subjects (here miners or developers) is even more difficult. It is quite unclear at the moment how a sensible sample of miners could be recruited. This is related to similar problems for sampling decision makers in software design.

4.2 Thwarting Long-Range Attacks with Peacock Mantis Shrimp Checkpoints

Sarah Azouvi (Protocol Labs – Edinburgh, GB), George Danezis (University College London, GB), Bryan Ford (EPFL Lausanne, CH), Philipp Jovanovic (University College London, GB), Pedro Moreno-Sanchez (IMDEA Software Institute – Madrid, ES), Joachim Neu (Stanford University, US), Tim Ruffing (Blockstream – Victoria, CA)

In this work, we propose Peacock Mantis Shrimp, a checkpointing mechanism onto Bitcoin for any PoS consensus scheme. It supports PoS schemes with an arbitrary number of validators, and has an efficient checkpoint verification requiring auditors to download only a small number of Bitcoin full blocks. Peacock Mantis Shrimp achieves this by randomly sampling validators into subgroups which then commit a previously agreed-upon checkpoint onto the Bitcoin blockchain using specially crafted threshold signed transactions. Peacock Mantis Shrimp improves on the state-of-the-art that either suffers from scaling constraints, supporting only a limited number of validators, or requires auditors to examine the full Bitcoin chain. We analyze parametrizations and show the overall failure probability can be driven as low as desired.

4.3 Cross-Chain Privacy

Jens Ernstberger (TU München, DE) and Fan Zhang (Yale University – New Haven, US)

Cross-Chain Communication received a lot of attention recently due to growing interoperability needs in DeFi and major security flaws in existing protocols that had caused significant financial loss for their users. This session came forth due to a recently published work, zkBridge [5], that improves the safety of cross-chain communication by replacing trusted committees (a single point failure) with zero-knowledge proofs (ZKP). While improving safety is crucial, the privacy implication of bridges received much less attention. Most deployed systems do not provide privacy guarantees and in particular allow an observer to *link* bridged assets to the original ones. Such linkage could affect the frangibility of assets (since minted coins inherit their history from the source chain) and even erode user privacy (e.g., deanonymization attacks on one chain could now impact other chains through bridges).

This article provides a summary proposed solutions for privacy-preserving, and discusses the opportunities and challenges. The discussion evolved around *(i)* the current solution space for privacy in cross-chain solutions, *(ii)* unique use-cases for private cross-chain communication, *(iii)* potential pitfalls in privacy preserving cross-chain solutions with regard to interoperability of private and public blockchains and *(iv)* alternatives to zkSNARK based solutions for private cross-chain bridges.

Generally, cross-chain exchanges of assets can be facilitated by either atomic swaps or bridges. (Here we leave sidechains (such as [6]) out of scope since we target solutions that can bridge two existing blockchains.) Depending on whether the source/destination blockchain provides native privacy guarantees, such exchanges can happen in one of the following scenarios:

1. public → public
2. public → private
3. private → public
4. private → private

Further, we find that the following (rather informal) privacy goals are essential – *(i)* hiding the fact that a swap/bridge of an asset takes place, *(ii)* hiding the amount / type of the involved asset and *(iii)* ensuring unlinkability between participants. We elaborate on privacy-preserving approaches to cross-chain communication that use atomic swaps and bridges, and in which scenarios each of them are applicable as well as sufficiently researched, in the following.

In an atomic swap, Alice intends to exchange X tokens A (native to blockchain A) for Y tokens B (native to blockchain B), such that the asset exchange is included atomically in both blockchains. Simply, this exchange can be achieved with HTLCs. However, HTLCs do not provide privacy, such that recent work proposed adaptor signatures to atomically release secrets whilst assuring privacy [1, 4]. However, we find that applying an atomic swap based on adaptor signatures inherently depends of the confidentiality of the underlying blockchain. Further, we find that such a construction only works if blockchain A is public (i.e. the transaction where the first transaction is included, case 1 + 2). If the sender blockchain is private (e.g., for shielded addresses in Zcash), there is no way to guarantee atomic inclusion in existing constructions. [4] suggests that that their method can be extended to shielded coins with 2PC generation of SNARKs, though details are not specified.

While atomic swaps allows a pair of users to exchange assets, a bridge can enable arbitrary message passing between two chains (thus atomic swaps can be seen as a specific application of a bridge). Typically bridges either depends on *(i)* a committee or *(ii)* a relayer network that relays the block header. Alternative approaches also provide cross-chain capabilities through TEEs and MPC [2, 3]. As the current state-of-the-art converges on a construction based on a relayer network, we discussed potential extensions to bridges in this domain. As a result, we find that bridges relying on a relayer with an updater contract are inherently incapable of obfuscating the fact that a bridging of assets took place. However, by applying a blockchain mixer on both the source and receiver chain, one can hide the amount transferred as well as provide unlinkability of sender and receiver accounts. Note, that a single mixer on the source chain is sufficient to ensure unlinkability, whereas a second mixer on the receiving chain can ensure confidentiality of the received amount by the receiver. Note that a private bridge is currently only possible for cross-chain communication between two public chains (Case 1), due to non-existent deployments of privacy-preserving smart contract enabled blockchains (which may change in the future).

In comparison, existing proposals for both private atomic swaps and private bridges face unique limitations that are partially exclusive. We also noted that performing generalized, privacy preserving smart contract function calls, where the invoked function resides on a different chain and the result of the function call needs to be returned to the invoker, can be especially challenging and is an equally unsolved problem, even in a case that involves no privacy. In general, it depends on the use-case at hand, whether one needs to apply a privacy preserving atomic swap or bridge. We deem further investigation of hybrid approaches, that leverage the benefits of both privacy preserving atomic swaps and bridges, an interesting area of future work.

References

1 A. Deshpande and M. Herlihy. *Privacy-preserving cross-chain atomic swaps*. In International Conference on Financial Cryptography and Data Security, 2020.

2 I. Leontiadis. *Private Blockchain Bridge*. Published in `https://hackmd.io/@EwNO7cCvQvylTn3mdYWOPQ/rk-r3kZOq`.

3 Y. Lan, J. Gao, Y. Li, K. Wang, Y. Zhu, and Z. Chen. *Trustcross: Enabling confidential interoperability across blockchains using trusted hardware*. In 4th International Conference on Blockchain Technology and Applications, 2021.

4 S. Thyagarajan, K. Aravinda, G. Malavolta, and P. Moreno-Sanchez. *Universal atomic swaps: Secure exchange of coins across all blockchains*. In IEEE Symposium on Security and Privacy, 2022.

5 T. Xie, J. Zhang, Z. Cheng, F. Zhang, Y. Zhang, Y. Jia, D. Boneh, and D. Song. *zkBridge: Trustless Cross-chain Bridges Made Practical*. Archiv, 2022.

6 F. Baldimtsi, I. Miers, and X. Zhang. *Anonymous Sidechains*. In Data Privacy Management, Cryptocurrencies and Blockchain Technology, 2022.

4.4 Longest Chain Consensus Under Low Bandwidth

Joachim Neu (Stanford University, US), Lucianna Kiffer (ETH Zürich, CH)

Traditionally, Nakamoto's longest chain (LC) consensus protocol is analyzed and proven secure in the synchronous adversarial Δ-bounded-delay network model. Specifically, analyses such as [1, 2, 3, 4, 5] exhibit the tradeoff between block production rate λ, adversarial resilience β, and delay upper bound Δ. Thus, these analyses examine 'how much honest mining rate is lost' because honest nodes mine on 'old' chains because they have not yet heard of the most recent chains due to the Δ delay.

However, the Δ-bounded-delay network model assumes that consensus messages travel between honest nodes with at most Δ delay, *irrespective of network load.* Thus, the model neglects important aspects of real communication networks such as congestion and queuing delays caused by limited bandwidth. Consequently, the prior analyses do not capture "how much honest mining rate is lost" because honest nodes mine on "old" chains while they are busy downloading more recent chains.

Earlier work [6] provides a network model that captures the fact that every node has limited bandwidth of C block content downloads per time, and analyzes proof-of-stake (PoS) Nakamoto consensus in that setting. For PoS LC, an analysis capturing a bandwidth constraint was particularly interesting, because in PoS the adversary can produce an infinite number of "valid" blocks for each block production opportunity, then spam the network with these equivocating blocks, and thus induce congestion in an attempt to attack the protocol. Though proof-of-work (PoW) LC naturally throttles the spamming ability of the adversary through the necessity of producing valid "work", the problem of congestion and block download delay remains relevant. In particular, we observe this when bandwidth is low (i.e., when target consensus throughput is close to the bandwidth limit).

Unfortunately, the analysis of [6] is rather pessimistic, in the sense that it analyses the worst-case amount of outstanding block downloads and provisions sufficiently high bandwidth C to always be able to complete outstanding downloads promptly. Consequently, the provisioned bandwidth C is asymptotically higher than average-case block download requirement based on the blockchain's throughput. As a result, the basic LC variant of [6] requires vanishing throughput for security, a situation that [6] only improves upon by proposing a parallel composition of multiple instances of the basic LC variant.

In contrast, in our group work we aimed to improve upon [6] and to show that both PoW and PoS Nakamoto consensus can be made secure for low (i.e., constant) bandwidth and thus for non-vanishing throughput. In the PoW setting, the global limit on block production rate provided by PoW can be used to strengthen the analysis of [6]. For PoS LC, further changes to the protocol are necessary to ensure that per block production opportunity, honest nodes need to download at most one block content. Specifically, in a new protocol, honest nodes could use the consensus protocol to agree on "proofs of equivocation" to consistently blank out the contents of equivocating blocks from the block tree and thus obviate the need to download multiple equivocating blocks. Thus, as compared to [6], a new protocol should maintain the structure of Nakamoto consensus, while providing security under non-vanishing throughput proportional to the bandwidth constraint.

References

1 R. Pass, L. Seeman, and a. shelat. *Analysis of the blockchain protocol in asynchronous networks*. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2017.

2 R. Pass and E. Shi. *The sleepy model of consensus*. In International Conference on the Theory and Application of Cryptology and Information Security, 2017.

3 L. Kiffer, R. Rajaraman, and a. shelat. *A better method to analyze blockchain consistency*. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018.

4 P. Gaži, A. Kiayias, and A. Russell. *Tight consistency bounds for bitcoin*. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020.

5 A. Dembo, S. Kannan, E. Tas, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni. *Everything is a race and nakamoto always wins*. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020.

6 J. Neu, S. Sridhar, L. Yang, D. Tse, and M. Alizadeh. *Securing Proof-of-Stake Nakamoto Consensus Under Bandwidth Constraint*. In AFT '22: 4th ACM Conference on Advances in Financial Technologies, 2022.

4.5 Stability in DeFi

Aviv Yaish (The Hebrew University of Jerusalem, IL), Alex Biryukov (University of Luxembourg, LU), Rainer Böhme (Universität Innsbruck, AT), Arthur Gervais (Imperial College London, GB), Lioba Heimbach (ETH Zürich, CH), Aljosha Judmayer (Universität Wien & SBA Research – Wien), Ben Livshits (Imperial College London, GB), Marie Vasek (University College London, GB), Roger Wattenhofer (ETH Zürich, CH)

Notions of Stability and Risk

Stability in traditional financial systems is not well-defined, though a common definition used by the European Central Bank [1] and the World Bank [2] treats economic stability as the ability of an economic ecosystem to sustain shocks while still continuing to function and providing financial services as usual.

This definition could be imported to the *Decentralized Finance* (*DeFi*) ecosystem. Although such definitions are still relevant, they ignore certain inherent properties of DeFi protocols and the underlying blockchain infrastructure. Certain platforms, such as *Constant Product Automated Market Makers* (*CPAMMs*) and utilization-based lending pools can continue functioning in times of duress, though in an unstable manner [3] where market prices violently oscillate in short periods of time [4]. Although users are traditionally viewed as promoting a more efficient market, their self-interested actions actually might cause price instability [5].

Types of DeFi Risk

From a technical viewpoint, there are three types of high level DeFi risks:
1. Ones that lead to the collapse or instability of one DeFi ecosystem or token.
2. Instability which starts with one DeFi ecosystem and propagates to another.
3. The risk that a collapse or instability propagates to the traditional financial system [7].

How Can DeFi Risks and Stability be Measured?

An encompassing definition of stability, although perhaps slightly imprecise, would be the ecosystem's proximity to a price equilibrium for all assets and financial services contained within the ecosystem [6].

When quantifying stability in the context of DeFi, due to the wildly varying mechanisms involved [11], one can take a per-platform approach. A potential avenue to explore is the requirements to trigger a "bank run" on lending protocols and how close these are to such a collapse. If cryptocurrency prices were to fall quickly and liquidations could no longer execute in time, lending pools that could no longer meet contractual obligations to repay lenders would face a liquidity crisis [12].

Burning the World Down: Destabilizing DeFi

Besides exploring and identifying already existing stability risks in DeFi protocols, another question is how can one design attacks on DeFi or use DeFi to execute attacks that amplify already existing problems such that suboptimality and inefficiencies are more likely to lead to instability.

Such attacks could be performed using a mixture of technical and financial means, for example Distributed Denial-of-Service (DDoS) attacks at the network level [10], or preventing oracle price updates by creating congestion [9].

Another attack strategy would be to synchronize the actions of multiple entities by technical means. Crowdfunded attacks could be executed directly on the consensus layer, as suggested in [8]. But also new attacks which utilize Blockscan messaging and smart contracts to manipulate interest rates, as demonstrated by [3] can be envisioned.

References

1 European Central Bank. *Financial stability and macroprudential policy*. In `https://www.ecb.europa.eu/ecb/tasks/stability/html/index.en.html`, last accessed 2022.

2 World Bank. *Financial stability*. In `https://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/financial-stability`, last accessed 2022.

3 A. Yaish, M. Dotan, K. Qin, A. Zohar, and A. Gervais. *Suboptimality in DeFi*, 2022.

4 M. Friedman. *A monetary and fiscal framework for economic stability*. In Essential Readings in Economics, Springer: 345-365, 1995.

5 N. Kaldor. *Speculation and economic stability*. In The Review of Economic Studies, Wiley-Blackwell, 7:1-27, 1939.

6 P. Samuelson. *Spatial price equilibrium and linear programming*. In The American Economic Review, JSTOR, 42:293-303. 1952.

7 S. Aramonte, W. Huang, and A. Schrimpf. *DeFi risks and the decentralisation illusion*. 2021.

8 A. Judmayer, N. Stifter, A. Zamyatin, I. Tsabary, I. Eyal, P. Gazi, S. Meiklejohn, and E. Weippl. *Pay to win: Cheap, crowdfundable, cross-chain algorithmic incentive manipulation attacks on PoW cryptocurrencies*. In Cryptology ePrint Archive, 2019.

9 B.Liu, P. Szalachowski, and J. Zhou. *A first look into defi oracles*. In IEEE International Conference on Decentralized Applications and Infrastructures, 2021.

10 R. Chaganti, R. Boppana, V. Ravi, K. Munir, M. Almutairi, F. Rustam, E. Lee, and I. Ashraf. *A Comprehensive Review of Denial of Service Attacks in Blockchain Ecosystem and Open Challenges*. In IEEE Access, 10:96538-96555, 2022.

11 F. Schär. *Decentralized Finance: On Blockchain-and Smart Contract-based Financial Markets*. In SSRN 3571335, 2021.

12 L. Gudgeon, D. Perez, D. Harz, B. Livshits, and A. Gervais. *The Decentralized Financial Crisis*. In Crypto Valley Conference on Blockchain Technology, 2020.

Participants

- Svetlana Abramova
Universität Innsbruck, AT
- Sarah Azouvi
Protocol Labs – Edinburgh, GB
- Alex Biryukov
University of Luxembourg, LU
- Rainer Böhme
Universität Innsbruck, AT
- Stefanos Chaliasos
Veridise – London, GB
- George Danezis
University College London, GB
- Markus Dürmuth
Leibniz Universität Hannover, DE
- Jens Ernstberger
TU München, DE
- Bryan Ford
EPFL Lausanne, CH
- Arthur Gervais
Imperial College London, GB
- Lioba Heimbach
ETH Zürich, CH
- Philipp Jovanovic
University College London, GB
- Aljosha Judmayer
Universität Wien & SBA Research – Wien
- Ghassan Karame
Ruhr-Universität Bochum, DE
- Lucianna Kiffer
ETH Zürich, CH
- Ben Livshits
Imperial College London, GB
- Pedro Moreno-Sanchez
IMDEA Software Institute – Madrid, ES
- Joachim Neu
Stanford University, US
- Tim Ruffing
Blockstream – Victoria, CA
- Florian Tschorsch
TU Berlin, DE
- Marie Vasek
University College London, GB
- Roger Wattenhofer
ETH Zürich, CH
- Aviv Yaish
The Hebrew University of Jerusalem, IL
- Fan Zhang
Yale University – New Haven, US
- Liyi Zhou
Chainlink Labs – London, GB
- Aviv Zohar
The Hebrew University of Jerusalem, IL