

Contents

CoDecFin – DeFi Risks

Risk Framework for Bitcoin Custody Operation with the Revault Protocol	3
<i>Jacob Swambo and Antoine Poinso</i>	
Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs	21
<i>Ryosuke Ushida and James Angel</i>	

CoDecFin – AML/KYC and Privacy

Collaborative Deanonymization	39
<i>Patrik Keller, Martin Florian, and Rainer Böhme</i>	
Re: FinCEN Docket Number FINCEN-2020-0020; RIN 1506-AB47; Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets	47
<i>Ryan Taylor</i>	
Analyzing FinCEN’s Proposed Regulation Relating to AML and KYC Laws	54
<i>Aaron Wright and Sachin Meier</i>	

DeFi – Protocol Design

Optimal Fees for Geometric Mean Market Makers	65
<i>Alex Evans, Guillermo Angeris, and Tarun Chitra</i>	
Market Based Mechanisms for Incentivising Exchange Liquidity Provision	80
<i>W. Gawlikowicz, B. Mannerings, T. Rudolph, and D. Šiška</i>	
Understand Volatility of Algorithmic Stablecoin: Modeling, Verification and Empirical Analysis	97
<i>Wenqi Zhao, Hui Li, and Yuming Yuan</i>	
Measuring Asset Composability as a Proxy for DeFi Integration	109
<i>Victor von Wachter, Johannes Rude Jensen, and Omri Ross</i>	

Demystifying Pythia: A Survey of ChainLink Oracles Usage on Ethereum	115
<i>Mudabbir Kaleem and Weidong Shi</i>	
On Stablecoin Price Processes and Arbitrage	124
<i>Ingolf Gunnar Anton Pernice</i>	
Red-Black Coins: Dai Without Liquidations	136
<i>Mehdi Salehi, Jeremy Clark, and Mohammad Mannan</i>	
DeFi – Formal Attack Analysis	
Formal Analysis of Composable DeFi Protocols	149
<i>Palina Tolmach, Yi Li, Shang-Wei Lin, and Yang Liu</i>	
How to Exploit a DeFi Project	162
<i>Xinyuan Sun, Shaokai Lin, Vilhelm Sjöberg, and Jay Jie</i>	
DeFi – Economics and Regulation	
DeFi as an Information Aggregator	171
<i>Jiasun Li</i>	
A Game-Theoretic Analysis of Cross-ledger Swaps with Packetized Payments	177
<i>Alevtina Dubovitskaya, Damien Ackerer, and Jiahua Xu</i>	
DeFi – MEV and Illicit Activity	
Wendy Grows Up: More Order Fairness	191
<i>Klaus Kursawe</i>	
Measuring Illicit Activity in DeFi: The Case of Ethereum	197
<i>Jiasun Li, Foteini Baldimtsi, Joao P. Brandao, Maurice Kugler, Rafeh Hulays, Eric Showers, Zain Ali, and Joseph Chang</i>	
DeFi – Order Routing and Formal Methods	
Global Order Routing on Exchange Networks	207
<i>Vincent Danos, Hamza El Khalloufi, and Julien Prat</i>	
Towards a Theory of Decentralized Finance	227
<i>Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente</i>	

Voting

Auditing Hamiltonian Elections	235
<i>Michelle Blom, Philip B. Stark, Peter J. Stuckey, Vanessa Teague, and Damjan Vukcevic</i>	
Cast-as-Intended: A Formal Definition and Case Studies	251
<i>Peter B. Rønne, Peter Y. A. Ryan, and Ben Smyth</i>	
Mobile Voting – Still Too Risky?	263
<i>Sven Heiberg, Kristjan Krips, and Jan Willemson</i>	
New Standards for E-Voting Systems: Reflections on Source Code Examinations	279
<i>Thomas Haines and Peter Roenne</i>	
Post-quantum Online Voting Scheme	290
<i>Guillaume Kaim, Sébastien Canard, Adeline Roux-Langlois, and Jacques Traoré</i>	
Short Paper: Ballot Secrecy for Liquid Democracy	306
<i>Mahdi Nejadgholi, Nan Yang, and Jeremy Clark</i>	
Shorter Lattice-Based Zero-Knowledge Proofs for the Correctness of a Shuffle	315
<i>Javier Herranz, Ramiro Martínez, and Manuel Sánchez</i>	
 WTSC – Security and Verification	
On-Chain Smart Contract Verification over Tendermint	333
<i>Luca Olivieri, Fausto Spoto, and Fabio Tagliaferro</i>	
Publicly Verifiable and Secrecy Preserving Periodic Auctions	348
<i>Hisham S. Galal and Amr M. Youssef</i>	
EthVer: Formal Verification of Randomized Ethereum Smart Contracts	364
<i>Łukasz Mazurek</i>	
Absentia: Secure Multiparty Computation on Ethereum	381
<i>Didem Demirag and Jeremy Clark</i>	
Empirical Analysis of On-chain Voting with Smart Contracts	397
<i>Robert Muth and Florian Tschorsch</i>	

WTSC – Foundations

Mirroring Public Key Infrastructures to Blockchains for On-Chain Authentication	415
<i>Ulrich Gellersdörfer, Friederike Groschupp, and Florian Matthes</i>	
Reactive Key-Loss Protection in Blockchains	431
<i>Sam Blackshear, Konstantinos Chalkias, Panagiotis Chatzigiannis, Riyaz Faizullahoy, Irakliy Khaburzaniya, Eleftherios Kokoris Kogias, Joshua Lind, David Wong, and Tim Zakian</i>	
Merkle Trees Optimized for Stateless Clients in Bitcoin	451
<i>Bolton Bailey and Suryanarayana Sankagiri</i>	
Soft Power: Upgrading Chain Macroeconomic Policy Through Soft Forks	467
<i>Dionysis Zindros</i>	
Privacy-Preserving Resource Sharing Using Permissioned Blockchains: (The Case of Smart Neighbourhood)	482
<i>Sepideh Avizheh, Mahmudun Nabi, Saoreen Rahman, Setareh Sharifian, and Reihaneh Safavi-Naini</i>	

WWTSC – Attacks’ Analysis

SoK: Algorithmic Incentive Manipulation Attacks on Permissionless PoW Cryptocurrencies	507
<i>Aljoshia Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Ittay Eyal, Peter Gaži, Sarah Meiklejohn, and Edgar Weippl</i>	
Pay to Win: Cheap, Cross-Chain Bribing Attacks on PoW Cryptocurrencies ...	533
<i>Aljoshia Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Ittay Eyal, Peter Gaži, Sarah Meiklejohn, and Edgar Weippl</i>	

WTSC – DeFi and Tokens

SoK: Lending Pools in Decentralized Finance	553
<i>Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente</i>	
Standardized Crypto-Loans on the Cardano Blockchain	579
<i>Dmytro Kondratiuk, Pablo Lamela Seijas, Alexander Nemish, and Simon Thompson</i>	
Fairness in ERC Token Markets: A Case Study of CryptoKitties	595
<i>Kentaro Sako, Shin’ichiro Matsuo, and Sachin Meier</i>	

Coins, Covid, Keynes and K-Shaped Recovery	611
<i>Pepi Martinez, William Huang, and Bud Mishra</i>	
Author Index	629