Category	Title	Authors	Affiliation
	Wed, 19 May 2021, 15:00-17:30 UTC		
Keynote	**Tim Roughgarden Title TBA**	Tim Roughgarden	Columbia University
A	Submission 142: Attacking the DeFi Ecosystem with Flash Loans for Fun an	Kaihua Qin; Liyi Zhou; Benjamin Livshits; Arthur Gervais	Imperial College London; Imperial College London;
A	Submission 157: FairMM: A Fast and Frontrunning-Resilient Crypto Market-	Michele Ciampi; Muhammad Ishaq; Malik Magdon-Ismail; Rafail Ostrovsky;	The University of Edinburgh; The University of Edir
A	Submission 148: Order-Fair Consensus for Blockchains	Mahimna Kelkar	Cornell Tech, Cornell University
	Wed, 26 May 2021, 15:00-17:30 UTC		
Keynote	**Ari Juels Title TBA**	Ari Juels	Cornell Tech
B	Submission 120: Blitz: Secure Multi-Hop Payments Without Two-Phase Com	Lukas Aumayr; Pedro Moreno-Sanchez; Aniket Kate; Matteo Maffei	TU Wien; IMDEA Software Institute; Purdue Univer
A	Submission 102: P2DEX: Privacy-Preserving Decentralized Cryptocurrency	Carsten Baum; Bernardo David; Tore Frederiksen	Aarhus University; IT University of Copenhagen; Al
B	Submission 112: Bitcoin-Compatible Virtual Channels	Lukas Aumayr; Oguzhan Ersoy; Andreas Erwig; Sebastian Faust; Kristina H	Technische Universität Wien; Delft University of Te
	Wed, 2 June 2021, 15:00-17:30 UTC		
Keynote	**Andreas Rossberg TBC**		DFINITY
H	Submission 127: A formal model of Algorand smart contracts	Massimo Bartoletti; Andrea Bracciali; Cristian Lepore; Alceste Scalas; Rober	University of Cagliari; University of Stirling; Univers
H	Submission 137: SciviK: A Versatile Framework for Specifying and Verifying	Shaokai Lin; Xinyuan Sun; Jianan Yao; Ronghui Gu	sl4299@columbia.edu; sxysun@certik.io; jy3022@
H	Submission 117: Accurate Smart Contract Verification Through Direct Model	Matteo Marescotti; Rodrigo Otoni; Leonardo Alt; Patrick Eugster; Antti E. J.	Università della Svizzera italiana; Università della
	Wed, 9 June 2021, 15:00-17:30 UTC		
Keynote	**Roger Wattenhofer TBA**	Roger Wattenhofer	ETH Zurich
G	Submission 124: MAD-HTLC: Because HTLC is Crazy-Cheap to Attack	Itay Tsabary; Matan Yechieli; Alex Manuskin; Ittay Eyal	Technion, IC3; Technion, IC3; ZenGo-X; Technion,
G	Submission 128: Reparo: Publicly Verifiable Layer to Repair Blockchains	Sri Aravinda Krishnan Thyagarajan; Adithya Bhat; Bernardo Magri; Daniel Ts	Friedrich Alexander Universität Erlangen-Nürnberg
E	Submission 150: Free2Shard: Identity-free sharding via Dynamic Self-allocat	Ranvir Rana; Sreeram Kannan; David Tse; Pramod Viswanath	University of Illinois at Urbana-Champaign; Univers
	Wed, 16 June 2021, 15:00-17:30 UTC		
Keynote	**Sara Tucci Title TBA**	Sara Tucci	CEA LIST
C	Submission 110: The Discriminating Miner Dilemma: Revisiting Liveness Gu	Fredrik Kamphuis; Bernardo Magri; Sebastian Faust	Robert Bosch GmbH; Aarhus University; Technical
C	Submission 121: A Rational Protocol Treatment of 51% Attacks	Christian Badertscher; Yun Lu; Vassilis Zikas	IOHK; University of Edinburgh; Purdue University
C	Submission 109: Post-Quantum Security of the Bitcoin Backbone and Quant	Alexandru Cojocaru; Juan Garay; Aggelos Kiayias; Fang Song; Petros Walld	Inria; Texas A&M University; University of Edinburg
	Wed, 23 June 2021, 15:00-17:30 UTC		
Keynote	**Ittai Abraham Title TBA**	Ittai Abraham	VMware
D	Submission 152: On the Anonymity Guarantees of Anonymous Proof-of-Stak	Markulf Kohlweiss; Varun Madathil; Kartik Nayak; Alessandra Scafuro	University of Edinburgh; North Carolina State Unive
D	Submission 116: BFT Protocol Forensics	Peiyao Sheng; Gerui Wang; Kartik Nayak; Sreeram Kannan; Pramod Viswar	UIUC; UIUC; Duke University; University of Washi
D	Submission 156: Achieving State Machine Replication without Honesty Assu	Conor McMenamin; Vanesa Daza; Matteo Pontecorvi	Universitat Pompeu Fabra; Universitat Pompeu Fal
	Wed, 30 June 2021, 15:00-17:30 UTC		
Keynote	**Giulia Fanti Title TBA**	Giulia Fanti	Carnegie Mellon University
E	Submission 108: GearBox: An Efficient UC Sharded Ledger Leveraging the	Bernardo David; Bernardo Magri; Christian Matt; Jesper Buus Nielsen; Danie	IT University of Copenhagen; Aarhus University; C
E	Submission 140: Ebb-and-Flow Protocols: A Resolution of the Availability-Fi	Joachim Neu; Ertem Nusret Tas; David Tse	Stanford University; Stanford University; Stanford U
E	Submission 123: On the Routing-Aware Peering against Network-Eclipse Att	Muoi Tran; Akshaye Shenoi; Min Suk Kang	National University of Singapore; National Universi
	Wed, 7 July 2021, 15:00-17:30 UTC		
Keynote	**NN**		
F	Submission 129: Lockable Signatures for Blockchains: Scriptless Scripts for	Sri Aravinda Krishnan Thyagarajan; Giulio Malavolta	Friedrich Alexander Universität Erlangen-Nürnberg
F	Submission 132: Differentially Private Mixing for Cryptocurrencies	Foteini Baldimtsi; Samuel D. Gordon; Ioanna Karantaidou; Mingyu Liang; Ma	George Mason University; George Mason Universit
F	Submission 143: Foundations of Ring Sampling	Viktoria Ronge; Christoph Egger; Russell W.F. Lai; Dominique Schröder; Ho	Friedrich-Alexander-Universität Erlangen-Nürnberg

Category Summary

4	A DeFi & frontrunning
2	B Side-channels
3	C Bitcoin & game theory
3	D Consensus
4	E Scaling & networking
3	F Privacy/cryptography
2	G Smart contracts & application layer
3	H Language/Formal methods

nburgh; Rensselaer Polytechnic Institute; UCLA; Purdue University

exandra Institute

chnology; Technische Universität Darmstadt; Technische Universität Darmstadt; ETH Zürich; Technische Universität Wien; IMDEA Software Institute; Technische Universität Darmstadt

ity of Stirling; Technical University of Denmark; University of Trento

columbia.edu; ronghui.gu@columbia.edu

, IC3

sity of Washington, Seattle; Stanford University; Stanford University

ersity; Duke University; North Carolina State University

bra, CYBERCAT - Center for Cybersecurity Research of Catalonia; NOKIA Bell Labs Nozay

Jniversity

ty of Singapore; KAIST

; Friedrich-Alexander-Universität Erlangen-Nürnberg; Friedrich-Alexander-Universität Erlangen-Nürnberg; Friedrich-Alexander-Universität Erlangen-Nürnberg; The Chinese University of Hong Kong