Dimitris Karakostas

✉ dimit.karakostas@gmail.com
dimkarakostas.com
Github ▪ Google Scholar ▪ LinkedIn

Education

2017–2021 (expected) **PhD in Computer Science**, *School of Informatics, University of Edinburgh*, Scotland, UK.
Research interests include decentralized asset management and the economics and social implications of decentralized financial systems. (Advisor: *Prof. Aggelos Kiayias*)

2010–2016 **Dipl.-Ing Electrical & Computer Engineering**, *National Technical University of Athens*, Greece.
Degree equivalence: *B.Eng in Electrical & Computer Engineering* and *M.Eng in Computer Science*
Thesis: *Probabilistic attacks against compressed encrypted protocols* (Advisor: *Prof. Aris Pagourtzis*)

Experience

Nov 2017 - present **Researcher**, *IOHK*, Remote.
Conducted research on the settlement layer of Proof-of-Stake blockchains, including the design of stake delegation in Cardano, and on mitigation techniques for 51% attacks against distributed ledgers.

Sep 2017 - Apr 2019 **Advisor**, *SignedBlock*, Remote.
Contributed on the design and development of blockchain systems for tracing data and physical assets.

Feb 2016 - Mar 2017 **Student Researcher**, *CryptoSec Lab, University of Athens*, Athens, Greece.
Investigated compression-based side-channel attacks both from a theoretical and engineering perspective. Developed the Rupture and CTX frameworks.

Apr 2015 - Feb 2016 **Software Engineer Working Student**, *Nokia*, Athens, Greece.
Improved product code health by building a Continuous Integration system, an internal dashboard, and a fault predictability tool, which were used by the software engineers.

Publications & Manuscripts

preprint '21 **Conclave: A Collective Stake Pool Protocol**
Dimitris Karakostas*, Aggelos Kiayias, Mario Larangeira

IEEE ICBC '21 **Securing Proof-of-Work Ledgers via Checkpointing**
Dimitris Karakostas*, Aggelos Kiayias
IEEE International Conference on Blockchain and Cryptocurrency 2021

FC '21 **Efficient State Management in Distributed Ledgers**
Dimitris Karakostas*, Nikos Karayannidis, Aggelos Kiayias
Financial Cryptography and Data Security 2021

SCN '20 **Account Management in Proof of Stake Ledgers**
Dimitris Karakostas*, Aggelos Kiayias, Mario Larangeira
Security and Cryptography for Networks 2020

TOKENOMICS '19 **Cryptocurrency Egalitarianism: A Quantitative Approach**
Dimitris Karakostas*, Aggelos Kiayias, Christos Nasikas, Dionysis Zindros
International Conference on Blockchain Economics, Security and Protocols, Paris, France, 2019

FC '19 **A Formal Treatment of Hardware Wallets**
Myrto Arapinis, Andriana Gkaniatsou, Dimitris Karakostas*, Aggelos Kiayias
Financial Cryptography and Data Security 2021

BH EU '16 **CTX: Eliminating BREACH with Context Hiding**
Dimitris Karakostas*, Aggelos Kiayias, Eva Sarafianou, Dionysis Zindros
Black Hat Europe, London, UK, 2016

BH ASIA '16 **Practical New Developments on BREACH**
Dimitris Karakostas*, Dionysis Zindros
Black Hat Asia, Singapore, 2016

* Author names are ordered alphabetically.

Teaching Assistance

2018-2021 **Blockchains & Distributed Ledgers**, *University of Edinburgh*, Scotland, UK.
(Undergraduate Course, School of Informatics) Gave lectures on blockchain programming on Ethereum and smart contracts, designed multiple assignments and exams, and set up a private Ethereum testnet which was used by over 200 students over 3 years.

2015 **Cryptography**, *National Technical University of Athens*, Greece.
(Undergraduate Course, Department of Electrical & Computer Engineering) Gave lectures on web security and blockchains, and prepared multiple semester exercises and their automatic graders.

Invited Talks

FOCODILE '21 **Efficient State Management in Distributed Ledgers**
Dimitris Karakostas*, Nikos Karayannidis, Aggelos Kiayias

Theory and Practice of Blockchains '20 **Securing Proof-of-Work Ledgers via Checkpointing**
Dimitris Karakostas*, Aggelos Kiayias

AtheCrypt '20 **Securing Proof-of-Work Ledgers via Checkpointing**
Dimitris Karakostas*, Aggelos Kiayias

CESC '19 **Cryptocurrency Egalitarianism: A Quantitative Approach**
Dimitris Karakostas*, Aggelos Kiayias, Christos Nasikas, Dionysis Zindros

BSides Athens '17 **Attacking IPv6 - A MitM IPv6 patch for Bettercap**
Dimitris Grigoriou, Dimitris Karakostas*, Dionysis Zindros

AtheCrypt '17 **CTX: Eliminating BREACH with Context Hiding**
Dimitris Karakostas*, Aggelos Kiayias, Eva Sarafianou, Dionysis Zindros

BSides Athens '16 **Rupture: Automating Cryptanalysis of HTTPS for AES Ciphers**
Dimitris Karakostas*, Eva Sarafianou, Dionysis Zindros

RWC '16 **New Developments in BREACH**
Dimitris Karakostas*, Aggelos Kiayias, Dionysis Zindros

AtheCrypt '16 **Probabilistic attacks against compressed encrypted protocols**
Dimitris Karakostas

Academic Service

Subreviewer AFT 2021, FC 2021, ACM AFT 2020, ACM CCS 2020, IEEE S&B 2020, IEEE TDSC 2020, ACM CCS 2019, IEEE S&P 2019, FC 2019, IEEE TDSC 2019, PENCIL 2019, PKC 2018, IEEE Blockchain 2018

Local Organizing PKC 2020

Skills

Languages English (Proficient), Greek (Native)

Prog. Languages Python, JavaScript, Solidity, C/C++, MySQL, Java

Other git, vim, LaTeX, WebDev (HTML5, CSS3, Django, Flask, Node.js, React), TLS, REST, Jenkins