

# Dimitris Karakostas

✉ [dimit.karakostas@gmail.com](mailto:dimit.karakostas@gmail.com)  
[dimkarakostas.com](https://www.dimkarakostas.com)  
Github ■ Google Scholar ■ LinkedIn

---

## Professional Experience

- Dec 2021 - present **Research Associate**, *University of Edinburgh*, Edinburgh, Scotland, UK.  
Researching the state of blockchain decentralization and mitigating long-range attacks and enhancing auditability in Proof-of-Stake ledgers.
- Nov 2017 - Aug 2021 **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.
- 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 **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 multiple software engineering teams.

---

## Education

- 2017–2021 **PhD in Computer Science**, *School of Informatics, University of Edinburgh*, Scotland, UK.  
Thesis: *Digital Asset Management via Distributed Ledgers*  
Advised by Prof. Aggelos Kiayias
- 2010–2016 **MEng Electrical & Computer Engineering**, *National Technical University of Athens*, Greece.  
Thesis: *Probabilistic attacks against compressed encrypted protocols*  
Advised by Prof. Aris Pagourtzis

---

## Teaching

### University Teacher

- Sep 2021 - Dec 2021, Sep 2022 - Dec 2022 **Blockchains and Distributed Ledgers**, *University of Edinburgh*, Scotland, UK.  
5 ECTS credits, SCQF Level 11, 10 SCQF credits.  
Teacher of the Year 2023 (Nominated), Edinburgh University Students' Association.

### Teaching Assistant

- 2018-2020 **Blockchains and Distributed Ledgers**, *University of Edinburgh*, Scotland, UK.  
2015 **Cryptography**, *National Technical University of Athens*, Greece.

---

## Publications & Manuscripts

- ACM CCS '24 **Blockchain Bribing Attacks and the Efficacy of Counterincentives**  
[Dimitris Karakostas\\*](#), Aggelos Kiayias, Thomas Zacharias  
2024 ACM SIGSAC Conference on Computer and Communications Security
- CANS '24 **Scalable and Lightweight State-Channel Audits**  
Christian Badertscher, Maxim Jourenko, [Dimitris Karakostas\\*](#), Mario Larangeira  
23<sup>rd</sup> International Conference on Cryptology And Network Security (CANS)
- CAAW@WWW '24 **Statistical Confidence in Mining Power Estimates for PoW Blockchains**  
Mary Milad, Christina Ovezik, [Dimitris Karakostas†](#), Daniel W. Woods  
3<sup>rd</sup> International Cryptoasset Analytics Workshop (2024)
- Springer '24 **The Security of Delegated Proof-of-Stake Wallet and Stake Pools**  
[Dimitris Karakostas\\*](#), Mario Larangeira  
Blockchains: A Handbook on Fundamentals, Platforms and Applications (Advances in Information Security book series)
- FC '24 **SoK: A Stratified Approach to Blockchain Decentralization**  
Christina Ovezik, [Dimitris Karakostas†](#), Aggelos Kiayias  
28<sup>th</sup> Financial Cryptography and Data Security (2024)

---

\* Author names are ordered alphabetically.

† Blockchain Technology Lab's author ordering policy: <https://www.ed.ac.uk/informatics/blockchain/btl-papers/aop>

- ACM AFT '22 **Blockchain Nash Dynamics and the Pursuit of Compliance**  
Dimitris Karakostas\*, Aggelos Kiayias, Thomas Zacharias  
 4<sup>th</sup> ACM Advances in Financial Technologies (2022)
- ACM MobiHoc '22 **Optimal Bootstrapping of PoW Blockchains**  
 Ranvir Rana, Dimitris Karakostas, Sreeram Kannan, Aggelos Kiayias, Pramod Viswanath  
 23<sup>rd</sup> ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for  
 Mobile Networks and Mobile Computing (2022)
- CBT@ESORICS '21 **Filling the Tax Gap via Programmable Money**  
Dimitris Karakostas\*, Aggelos Kiayias  
 5<sup>th</sup> International Workshop on Cryptocurrencies and Blockchain Technology (2021)
- ESORICS '21 **Conclave: A Collective Stake Pool Protocol**  
Dimitris Karakostas\*, Aggelos Kiayias, Mario Larangeira  
 26<sup>th</sup> European Symposium on Research in Computer Security (2021)
- IEEE ICBC '21 **Securing Proof-of-Work Ledgers via Checkpointing**  
Dimitris Karakostas\*, Aggelos Kiayias  
 3<sup>rd</sup> IEEE International Conference on Blockchain and Cryptocurrency (2021)
- FC '21 **Efficient State Management in Distributed Ledgers**  
Dimitris Karakostas\*, Nikos Karayannidis, Aggelos Kiayias  
 25<sup>th</sup> Financial Cryptography and Data Security (2021)
- SCN '20 **Account Management in Proof of Stake Ledgers**  
Dimitris Karakostas\*, Aggelos Kiayias, Mario Larangeira  
 12<sup>th</sup> Security and Cryptography for Networks (2020)
- TOKENOMICS '19 **Cryptocurrency Egalitarianism: A Quantitative Approach**  
Dimitris Karakostas\*, Aggelos Kiayias, Christos Nasikas, Dionysis Zindros  
 1<sup>st</sup> International Conference on Blockchain Economics, Security and Protocols (2019)
- FC '19 **A Formal Treatment of Hardware Wallets**  
 Myrto Arapinis, Andriana Gkaniatsou, Dimitris Karakostas\*, Aggelos Kiayias  
 23<sup>rd</sup> Financial Cryptography and Data Security (2019)
- 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)

---

## Selected 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
- 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

Program Committee	CANS 2024, MARBLE 2022-24, CIFRIS 2023, TOKENOMICS 2022-23, BLOCKCHAIN 2022
Subreviewer	Crypto 2022, IEEE ICDCS 2022, IEEE Euro S&P 2021, ACM AFT 2020-21, FC 2019/2021, ACM CCS 2019-20, IEEE S&B 2020, IEEE S&P 2019, PENCIL 2019, PKC 2018, IEEE Blockchain 2018
Journal Reviewer	Journal of Computer and System Sciences 2023, IEEE Transactions on Dependable and Secure Computing 2019/2020
Local Organizing	PKC 2020

---

## Skills

Languages	Greek (Native), English (Proficient), German (Intermediate)
Programming	Python, JavaScript, Solidity, git, vim, HTML5/CSS3, Django, Flask, Node.js, React, TLS, REST