

Dionysis Zindros

✉ dionyziz@gmail.com
dionyziz.com ▪ github.com/dionyziz ▪ [Google Scholar](https://scholar.google.com/citations?user=...)

Education

- Oct 2021–Oct 2023 **Post-doctoral Scholar**, *Stanford University, USA*.
Conducted consensus and blockchain research with graduate and undergraduate students at David Tse's lab. Designed from scratch and taught 80% of the graduate course "EE374: Blockchain Foundations", involving heavy programming problem sets, for two consecutive academic years. Managed a \$4.5M private grant from IOG. Supervised multiple undergraduate theses.
- Apr 2020–Oct 2020 **Post-doctoral Researcher**, *Department of Informatics, University of Athens, Greece*.
Conducted consensus and blockchain research. Supervised undergraduate theses.
- 2015–2020 **PhD in Computer Science**, *Department of Informatics, University of Athens, Greece*.
Research Areas: Cryptography, Blockchains
Dissertation: *Decentralized Blockchain Interoperability*
Advised by Prof. Aggelos Kiayias
- 2008–2015 **MEng Electrical & Computer Engineering**, *National Technical University of Athens, Greece*.
Thesis: *Creating OpenBazaar: Trust in Decentralized Anonymous Marketplaces*
Advised by Prof. Aris Pagourtzis

Professional Experience

- Oct 2021–present **Founder**, *Common Prefix, Tallinn, Estonia & Athens, Greece*.
Created and managed blockchain consulting company offering auditing, cryptography and security services to the private sector with 10 active customers, 23 employees (of which 13 full-time), and \$1.7M in annual revenue.
- 2015–2020 **Research Assistant**, *Department of Informatics, University of Athens, Greece*.
Conducted research with public (ERC) and private funding (IOHK). Independently raised private funding (FrostWire, OB1). Published 16 papers with 220 citations. Supervised 13 theses leading to 7 publications. Worked closely with IOHK engineers to implement production blockchain systems (*Cardano, Midnight*).
- 2019–2020 **Co-Founder**, *SignedBlock, Athens, Greece*.
Created and managed blockchain consulting company offering smart contract and education services to the private sector with 5-6 employees and customers such as the National Bank of Greece. Developed subsecond frequency proprietary algorithmic trading strategies for cryptocurrencies.
- 2014–2015 **Software Engineer**, *Google, Zürich, Switzerland*.
Improved corporate security by building forensics and security tools used by the Google Incident Response and corporate network monitoring teams.
- 2013–2014 **Product Security Intern**, *Twitter, San Francisco, USA*.
Identified vulnerable endpoints and recommended mitigations in the areas of *BREACH* and *CSP*.
- 2010–2011 **Co-Founder, Technical Lead**, *Kamibu, Athens, Greece*.
Gaming software company. Raised seed round of \$70,000 to create *WebGL* game engine.
- 2006–2008 **Backend Software Engineer**, *deviantART, Los Angeles, USA*.
Community with 50,000,000 daily hits, 15,000,000 users. Wrote 200,000 lines of *PHP* and 5,000 of *MySQL* backend code. Leveraged *memcached*, sharding, and partitioning to improve performance and scalability.
- 2005–2010 **Co-Founder, Technical Lead**, *Zino, Athens, Greece*.
Greek social network with 20,000 members. Created over 300,000 lines of *PHP*, *JavaScript*, *HTML/CSS*, *XML/XSLT* code and supervised 5 programmers.

Publications & Manuscripts

- Preprint '24 **Blink: An Optimal Proof of Proof-of-Work**
Lukas Aumayr, Zeta Avarikioti, Matteo Maffei, Giulia Scaffino, [Dionysis Zindros](#)*

* Author names are ordered alphabetically.

- Preprint '24 **ROLLERBLADE: Replicated Distributed Protocol Emulation on Top of Ledgers**
[Dionysis Zindros](#), Apostolos Tzinas, David Tse
- Preprint '24 **A Better Proof-of-Work Fork Choice Rule**
Karl Kreder, Shreekara Shastry, Apostolos Tzinas, Sriram Vishwanath, [Dionysis Zindros*](#)
- FC '24 **Light Clients for Lazy Blockchains**
Ertem Nusret Tas, [Dionysis Zindros](#), Lei Yang, David Tse
Financial Cryptography 2024
- FC '24 **On-Chain Timestamps Are Accurate**
Apostolos Tzinas, Srivatsan Sridhar, [Dionysis Zindros](#)
Financial Cryptography 2024
- Preprint '23 **Better Safe than Sorry: Recovering after Adversarial Majority**
Srivatsan Sridhar, [Dionysis Zindros](#), and David Tse
- FC WTSC '23 **The Principal-Agent Problem in Liquid Staking**
Apostolos Tzinas, [Dionysis Zindros](#)
Financial Cryptography Workshop on Trusted Smart Contracts 2023
- FC WTSC '23 **Cassiopeia: Practical On-Chain Witness Encryption**
Schwinn Saereesitthipitak, [Dionysis Zindros](#)
Financial Cryptography Workshop on Trusted Smart Contracts 2023
- AFT '23 **Proofs of Proof-of-Stake with Sublinear Complexity**
Shresth Agrawal, Joachim Neu, Ertem Nusret Tas, [Dionysis Zindros*](#)
ACM Advances in Financial Technologies 2023
- FC WTSC '22 **Hours of Horus: Keyless Cryptocurrency Wallets**
[Dionysis Zindros](#)
Financial Cryptography Workshop on Trusted Smart Contracts 2022
- AFT '21 **The Velvet Path to Superlight Blockchain Clients**
Aggelos Kiayias, Andrianna Polydouri, [Dionysis Zindros*](#)
ACM Advances in Financial Technologies 2021
- CCS '21 **Mining in Logarithmic Space**
Aggelos Kiayias, Nikos Leonardos, [Dionysis Zindros*](#)
ACM Computer and Communications Security 2021
- FC '21 **SoK: Communication Across Distributed Ledgers**
Alexei Zamyatin, Mustafa Al-Bassam, [Dionysis Zindros](#), Eleftherios Kokoris-Kogias,
Pedro Moreno-Sanchez, Aggelos Kiayias, William J Knottenbelt
Financial Cryptography and Data Security 2021
- FC '21 **BRICK: Asynchronous Payment Channels**
Georgia Avarikioti, Eleftherios Kokoris Kogias, Roger Wattenhofer, [Dionysis Zindros*](#)
Financial Cryptography and Data Security 2021
- FC WTSC '21 **Soft Power: Upgrading Chain Macroeconomic Policy Through Soft Forks**
[Dionysis Zindros](#)
Financial Cryptography Workshop on Trusted Smart Contracts 2021
- AFT '20 **A Gas-Efficient Superlight Bitcoin Client in Solidity**
Stelios Daveas, Kostis Karantias, Aggelos Kiayias, [Dionysis Zindros*](#)
ACM Advances in Financial Technologies 2020
- ESORICS '20 **Updatable Blockchains**
Michele Ciampi, Nikos Karayannidis, Aggelos Kiayias, [Dionysis Zindros*](#)
ESORICS 2020
- FC '20 **Non-Interactive Proofs of Proof-of-Work**
Aggelos Kiayias, Andrew Miller, [Dionysis Zindros*](#)
Financial Cryptography and Data Security, Malaysia, 2020
- FC '20 **Proof-of-Burn**
Kostis Karantias, Aggelos Kiayias, [Dionysis Zindros*](#)
Financial Cryptography and Data Security, Malaysia, 2020
- MARBLE '20 **Smart Contract Derivatives**
Kostis Karantias, Aggelos Kiayias, [Dionysis Zindros*](#)
Mathematical Research for Blockchain Economy 2020

- S&P '19 **Proof-of-Stake Sidechains**
Peter Gaži, Aggelos Kiayias, [Dionysis Zindros*](#)
IEEE Symposium on Security and Privacy, San Francisco, USA, 2019
- FC WTSC '19 **Proof-of-Work Sidechains**
Aggelos Kiayias, [Dionysis Zindros*](#)
Financial Cryptography Workshop on Trusted Smart Contracts, St.Kitts & Nevis, 2019
- 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
- MARBLE '19 **Compact Storage of Superblocks for NIPoPoW Applications**
Kostis Karantias, Aggelos Kiayias, Nikos Leonardos, [Dionysis Zindros*](#)
Mathematical Research for Blockchain Economy, Santorini, Greece, 2019
Nominated for Best Paper Award
- arXiv Preprint 2018 **Structure and Content of the Visible Darknet**
Zeta Avarikioti, Roman Brunner, Aggelos Kiayias, Roger Wattenhofer, [Dionysis Zindros*](#)
- FC '17 **Trust Is Risk: A Decentralized Financial Trust Platform**
Orfeas Stefanos Thyfronitis Litos, [Dionysis Zindros*](#)
Financial Cryptography and Data Security, Malta, 2017
- 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

Teaching

Lecturing

- Winter 2023 **EE374: Blockchain Foundations**, *Stanford University, USA.*
[Dionysis Zindros](#), Prof. David Tse
Designed from scratch and taught 80% of this graduate-level course.
- Spring 2022 **EE374: Blockchain Foundations**, *Stanford University, USA.*
[Dionysis Zindros](#), Prof. David Tse
Designed from scratch and taught 80% of this graduate-level course.
- Spring 2019 **Blockchain Science and Engineering**, *University of Athens, Greece.*
Prof. Aggelos Kiayias. Additional Lecturing: Christos Nasikas, [Dionysis Zindros](#)
Graduate Course, Department of Computer Science
- Spring 2017 **Security of Computer Systems**, *University of Athens, Greece.*
Dr. Dimitris Mitropoulos. Additional Lecturing: Dionysis Zindros
Undergraduate and Graduate Courses, Department of Computer Science
- Spring 2016 **Security of Computer Systems**, *University of Athens, Greece.*
Prof. Aggelos Kiayias. Additional Lecturing: Yannis Tselekounis, [Dionysis Zindros](#)
Undergraduate and Graduate Courses, Department of Computer Science
- Fall 2015 **Cryptography**, *National Technical University of Athens, Greece.*
Prof. A. Pagourtzis & S. Zachos. Additional Lecturing: A. Antonopoulos, P. Grontas, P. Potikas, [D. Zindros](#)
Undergraduate Course, Department of Computer Engineering
- Fall 2010 **Introduction to Web Development**, *National Technical University of Athens, Greece.*
Petros Angelatos, Dionysis Zindros. 52-hour Extracurricular Undergraduate Seminar

Teaching Assistant

- Fall 2014 **Cryptography**, *National Technical University of Athens, Greece.*
Undergraduate Course, Department of Electrical & Computer Engineering
- Fall 2012 **Algorithms and Complexity**, *National Technical University of Athens, Greece.*
Undergraduate Course, Department of Electrical & Computer Engineering

Spring 2011 **Discrete Mathematics**, *National Technical University of Athens*, Greece.
Undergraduate Course, Department of Electrical & Computer Engineering

Olympiad Coach

2017 Balkan Olympiad in Informatics

2012, 2015 Junior Balkan Olympiad in Informatics

2010–12, 2015–16 National Greek Olympiad in Informatics

Students Advised

Summer Intern '22 Schwinn Saereesitthipitak, *Cassiopeia: Practical On-Chain Witness Encryption* [FC WTSC '23]
MSc Thesis '20 Andrianna Polydouri, *Non-Interactive Proofs of Proof-of-Work under Velvet Forks*
MSc Thesis '20 Stelios Daveas, *Gas-Efficient Verification of Non-Interactive Proofs of Proof-of-Work* [AFT '20]
MEng Thesis '19 Kostis Karantias, *Enabling NIPoPoW Applications on Bitcoin Cash* [MARBLE '19]
MSc Thesis '19 Orestis Konstantinidis, *Monero Mining: CryptoNight Analysis*
BSc Thesis '18 Roman Brunner, *Structure and Content of the Visible Darknet*
MEng Thesis '18 Giorgos Christoglou, *Enabling crosschain transactions using NIPoPoWs*
BSc Thesis '18 Dimitris Grigoriou, *Extending Compression Attack Frameworks Against Real Systems*
BSc Thesis '17 Christos Porios, *A bcoin.js Implementation of Trust-is-Risk*
MEng Thesis '17 Orfeas Stefanos Thyfronitis Litos, *Trust is Risk* [FC '17]
MEng Thesis '17 Eva Sarafianou, *Tool for cryptographic compression side channel attacks against TLS* [RWC '17]
MEng Thesis '16 K. Andrikopoulos & D. Kolotouros, *Multi-Party Off-the-Record Messaging Implementation*
MEng Thesis '16 Dimitris Karakostas, *Optimizations on Compression–Encryption Attacks against TLS* [BH ASIA '16]

Selected Invited Talks

ATHECRYPT '18 **Proofs of Proof-of-Work: Overview and Research Directions**
RWC '17 **Productizing TLS Attacks: The Rupture API**
Aggelos Kiayias, Eva Sarafianou, [Dionysis Zindros*](#)
RWC '16 **New Developments in BREACH**
Dimitris Karakostas, Aggelos Kiayias, [Dionysis Zindros*](#)
BSides Athens '16 **Rupture: Automating Cryptanalysis of HTTPS for AES Ciphers**
Dimitris Karakostas, Eva Sarafianou, [Dionysis Zindros*](#)
ECESCON '14 **HTTPS BREACH**
Keynote speaker

Professional Service

Program Committee AFT SIB 2024, SBC 2024, FC 2023, AFT 2021, FC 2021, FC WTSC 2021, MIT Cryptoeconomic Systems 2020, MARBLE 2020, FC WTSC 2020, IEEE Blockchain 2018
Subreviewer CANS 2024, SBC 2022, PODC 2021, EUROCRYPT 2021, CCS 2020, S&P 2020, CCS 2019, S&P 2019, TCC 2018, PoPETs 2018, FC BITCOIN 2018, CANS 2017, FC 2017, PoPETs 2017, EUROCRYPT 2016, DCCL 2016

Honors & Awards

2017–2020 IOHK Junior Research Fellowship

2006 Balkan Olympiad in Informatics Bronze Medal

Skills

Languages English (proficient), Greek (native), German (beginner)
Prog. Languages Python, JavaScript, TypeScript, C/C++, PHP, MySQL, \LaTeX
Other git, vim, TLS, OpenGL/WebGL, IRC, Linux Administration (Debian, Arch, Gentoo)