# Benedikt Bünz

✉ benedikt@cs.stanford.edu • 🖱 bue.nz

## Academic

**Courant Institute NYU** — **New York City, New York**
*Assistant Professor Computer Science, Tenure Track* — *From 2023/9*
Research Areas: Applied Cryptography, Blockchains

**Stanford University** — **Stanford, California**
*PhD in Computer Science, Advised by Dan Boneh* — *2016/9 – 2023/3*
Thesis: Improving the Privacy, Scalability, and Ecological Impact of Blockchains

**Stanford University** — **Stanford, California**
*MS in Computer Science* — *2014/9 – 2016/6*
Specializations: Artificial Intelligence and Theoretical CS

**University of Zurich** — **Zurich, Switzerland**
*BS in Computer Science, Summa cum laude* — *2011/9 – 2014/8*
Bachelor Thesis: Faster Algorithms and Better Payment Rules for Core-Selecting Combinatorial Auctions

## Work Experience

### Research Positions

**Espresso Systems** — **San Francisco, California**
*Cofounder and Chief Scientist* — *Since 2021/1*

**Visa Research** — **Palo Alto, California**
*Intern, PhD Summer Intern* — *6/17 to 9/17*
Confidential Smart Contracts

**University of Zurich** — **Zurich, Switzerland**
*Research Internship, Computing BNEs in Combinatorial Auctions* — *Summer '15*
Advised by Sven Seuken and Ben Lubin

**Stanford University** — **Stanford, California**
*Research Assistant, Provisions* — *Spring '15*
Dan Boneh

### Teaching Positions

**Stanford University** — **Stanford, California**
*Instructor, Cryptocurrencies and Blockchain Technologies (CS 251)* — *Fall '20 and '21*
Co-taught with Dan Boneh

**Stanford University** — **Stanford, California**
*Teaching Assistant, Cryptography (CS 255)* — *Winter '16*
Taught by Dan Boneh

**Stanford University** — **Stanford, California**
*Teaching Assistant, Bitcoin and Cryptocurrencies (CS 251)* — *Fall '15*
Taught by Dan Boneh and Joseph Bonneau

**University of Zurich** — **Zurich, Switzerland**
*Teaching Assistant, Combinatorial Auctions* — *Spring '14*
Taught by Sven Seuken

## Awards and Scholarships

**VeChain** **Stanford, California**
*Graduate Fellowship* *2020/9*
Supporting PhD Studies

**Microsoft** **Berkeley, California**
*Research Fellow at Simons Institute* *2019/9*
Proofs, Consensus and Decentralization workshop

**Studienstiftung des Deutschen Volkes** **Bonn, Germany**
*Auslandsstipendium, International studies scholarship* *2014/8*
35,000 EUR grant from the German Academic Scholarship Foundation

**Zühlke Technology Group AG** **Schlieren, Switzerland**
*Graduate studies scholarship, zuehlke.com* *2014/8*
9,000 CHF

**University Zurich** **Zurich, Switzerland**
*Semester Price, uzh.com* *2015/4*
Best 30 thesis per semester

**German Academic Scholarship Foundation** **Studienstiftung des Deutschen Volkes**
*2016/6, Bonn, Germany* *2012/9*
studienstiftung.de

Awarded to top 0.5% of German students

## Publications

### Publication Highlights and Summary

- Bulletproofs [Bün+18] is used in 4 Billion USD currency Monero[1] reducing tx fees by 80%. Also used by JP Morgan Chase[2] and other blockchains.
- Verifiable Delay Functions[Bon+18] are currently used by the 'green' cryptocurrency Chia[3] and are planned for Ethereum 2.0[4], Filecoin and others. There also exists an industry wide VDF alliance[5] that is funding research on VDF and VDF hardware development.
- 6 publications at top cryptography conferences (CRYPTO, EUROCRYPT, ASIACRYPT, TCC)
- 4 publications at top security conferences (IEEE S&P, CCS)
- 6 publications at top AI and EconCS conferences (AAAI, IJCAI, ICLR, EC, JAIR, ISR)

### Cryptography and Security (EUROCRYPT,CRYPTO and TCC are alphabetical)

[Bün+22] **Bünz**, B., Chen, B., Boneh, D., Zhang, Z., "HyperPlonk: Plonk with Linear-Time Prover and High-Degree Custom Gates". In: *IACR Cryptol. ePrint Arch.* (2022).

[BF22] **Bünz**, B., Fisch, B., "Schwartz-Zippel for multilinear polynomials mod N". In: *IACR Cryptol. ePrint Arch.* (2022).

[1] https://web.getmonero.org/resources/moneropedia/bulletproofs.html
[2] https://www.coindesk.com/business/2019/05/28/jpmorgan-adds-privacy-features-to-ethereum-based-quorum-blockch
[3] https://finance.yahoo.com/news/chia-network-153251783.html
[4] https://slideslive.com/38911623/ethereum-20-randomness
[5] https://www.vdfalliance.org/

[Xio+22] Xiong, A. L., Chen, B., Zhang, Z., **Bünz**, B., Fisch, B., Krell, F., Camacho, P., “VERI-ZEXE: Decentralized Private Computation with Universal Setup”. In: *IACR Cryptol. ePrint Arch.* (2022).

[Bün+21a] **Bünz**, B., Chiesa, A., Lin, W., Mishra, P., Spooner, N., “Proof-Carrying Data Without Succinct Arguments”. In: *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*. Ed. by Tal Malkin and Chris Peikert. Lecture Notes in Computer Science. Springer, 2021. eprint: https://eprint.iacr.org/2020/1618.

[Bün+21b] **Bünz**, B., Maller, M., Mishra, P., Tyagi, N., Vesely, P., “Proofs for inner pairing products and applications”. In: *Asiacrypt*. Lecture Notes in Computer Science. 2021. eprint: https://eprint.iacr.org/2019/1229.

[Bün+20a] **Bünz**, B., Agrawal, S., Zamani, M., Boneh, D., “Zether: Towards Privacy in a Smart Contract World”. In: *Financial Cryptography and Data Security - 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10-14, 2020 Revised Selected Papers*. Ed. by Joseph Bonneau and Nadia Heninger. Lecture Notes in Computer Science. Springer, 2020. eprint: https://eprint.iacr.org/2019/191.

[Bün+20b] **Bünz**, B., Chiesa, A., Mishra, P., Spooner, N., “Recursive Proof Composition from Accumulation Schemes”. In: *Theory of Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part II*. Ed. by Rafael Pass and Krzysztof Pietrzak. Lecture Notes in Computer Science. Springer, 2020. eprint: https://eprint.iacr.org/2020/499.

[BFS20] **Bünz**, B., Fisch, B., Szepieniec, A., “Transparent SNARKs from DARK Compilers”. In: *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I*. Ed. by Anne Canteaut and Yuval Ishai. Lecture Notes in Computer Science. Springer, 2020. eprint: https://eprint.iacr.org/2019/1229.

[Bün+20c] **Bünz**, B., Kiffer, L., Luu, L., Zamani, M., “FlyClient: Super-Light Clients for Cryptocurrencies”. In: *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*. IEEE, 2020. eprint: https://eprint.iacr.org/2019/226.

[BBF19] Boneh, D., **Bünz**, B., Fisch, B., “Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains”. In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Lecture Notes in Computer Science. Springer, 2019. eprint: https://eprint.iacr.org/2018/1188.

[Bon+18] Boneh, D., Bonneau, J., **Bünz**, B., Fisch, B., “Verifiable Delay Functions”. In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I*. Ed. by Hovav Shacham and Alexandra Boldyreva. Lecture Notes in Computer Science. Springer, 2018. eprint: https://eprint.iacr.org/2018/601.

[Bün+18] **Bünz**, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G., “Bulletproofs: Short Proofs for Confidential Transactions and More”. In: *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA*. IEEE Computer Society, 2018. eprint: https://eprint.iacr.org/2017/1066.

[BGB17] **Bünz**, B., Goldfeder, S., Bonneau, J., “Proofs-of-delay and randomness beacons in ethereum”. In: *IEEE Security and Privacy on the blockchain (IEEE S&B)* (2017). eprint: http://stevengoldfeder.com/papers/BGB17-IEEESB-proof_of_delay_ethereum.pdf.

[Dag+15] Dagher, G. G., **Bünz**, B., Bonneau, J., Clark, J., Boneh, D., “Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges”. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-16, 2015*. Ed. by Indrajit Ray, Ninghui Li, and Christopher Kruegel. ACM, 2015. eprint: `https://crypto.stanford.edu/~dabo/pubs/abstracts/provisions.html`.

### Artificial Intelligence

[Sel+19] Selsam, D., Lamm, M., **Bünz**, B., Liang, P., Moura, L., Dill, D. L., “Learning a SAT Solver from Single-Bit Supervision”. In: *7th International Conference on Learning Representations, ICLR 2019, New Orleans, LA, USA, May 6-9, 2019*. OpenReview.net, 2019. eprint: `https://arxiv.org/abs/1802.03685`.

### Economics and Computation

[BLS21] **Bünz**, B., Lubin, B., Seuken, S., “Computing Bayes-Nash Equilibria in Combinatorial Auctions with Verification”. In: *Information Systems Research (ISR) - Special Issue on Market Design and Analytics* (2021). Forthcoming. eprint: `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3178454`.

[Bos+20] Bosshard, V., **Bünz**, B., Lubin, B., Seuken, S., “Computing Bayes-Nash Equilibria in Combinatorial Auctions with Verification”. In: *J. Artif. Intell. Res.* (2020). eprint: `https://arxiv.org/abs/1812.01955`.

[BLS18] **Bünz**, B., Lubin, B., Seuken, S., “Designing Core-selecting Payment Rules: A Computational Search Approach”. In: *Proceedings of the 2018 ACM Conference on Economics and Computation, Ithaca, NY, USA, June 18-22, 2018*. Ed. by Éva Tardos, Edith Elkind, and Rakesh Vohra. ACM, 2018. eprint: `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3178454`.

[Bos+17] Bosshard, V., **Bünz**, B., Lubin, B., Seuken, S., “Computing Bayes-Nash Equilibria in Combinatorial Auctions with Continuous Value and Action Spaces”. In: *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI 2017, Melbourne, Australia, August 19-25, 2017*. Ed. by Carles Sierra. ijcai.org, 2017. eprint: `https://arxiv.org/abs/1812.01955`.

[BSL15] **Bünz**, B., Seuken, S., Lubin, B., “A Faster Core Constraint Generation Algorithm for Combinatorial Auctions”. In: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence, January 25-30, 2015, Austin, Texas, USA*. Ed. by Blai Bonet and Sven Koenig. AAAI Press, 2015. eprint: `http://www.aaai.org/ocs/index.php/AAAI/AAAI15/paper/view/10033`.

## Academic Service

- PC Co-Chair Stanford Blockchain Conference 2020 and 2019
- CCS 2021 PC Member
- AFT 2021 PC Member
- FC 2020 PC Member
- Scaling Bitcoin 2018 and 2017 PC Member
- ZK Proofs 2020 PC Member
- Subreviewer Eurocrypt, IndoCrypt, Asiacrypt, Crypto, IEEE S&P, CCS, and others

## Patents

**E.P. Patent No. EP3665858A4** **Pending**
*Verification of interactions system and method* *Assigned to Visa*

**U.S. Patent No. US20190164153A1** **Pending**
*Blockchain system for confidential and anonymous smart contracts* *Assigned to Visa and Stanford*

**U.S. Patent No. US20200252221A1** **Pending**
*Optimizations for verification of interactions system and method* *Assigned to Visa and Stanford*

## Talks

### Invited Talks and Lectures

1. Off-chain payment channels and the lightning network, CS 251, Stanford, November 2016
2. State of Crypto, Scaling Bitcoin, November 2017
3. Research in Cryptocurrencies, Café Scientifique, Stanford Blood Center, March 2018
4. Introduction to Blockchain, New Era of Economy- Blockchain technology, April 2018
5. Zero Knowledge in Cryptocurrency, Stanford Blockchain Club, May 2018
6. Non-PoW Consensus Approaches, Blockchain and CryptoEconomics, Berkeley University, October 2018
7. Cryptography for Cryptocurrencies, Enterprise Ethereum Alliance, March 2020
8. Privacy in Cryptocurrencies, Demystifying Big Data and FinTech, Cornell Graduate School of Management, October 2020
9. Zero Knowledge, Blockchain Seminar, NTU Singapore, October 2020
10. Intro to ZK proofs, ExpoLab Blockchain Speaker Series, November 2020
11. Zero Knowledge, Berkeley Defi Course, Berkeley University, May 2021

### Bulletproofs

12. **IEEE S&P (Oakland), May 2018**
13. Silicon Valley Ethereum Meetup, SV Ethereum Meetup, December 2017
14. Security Seminar, UCL, December 2017
15. BPASE Conference, Stanford Blockchain Center, January 2018
16. Cornell Tech Security Seminar, March 2018
17. Bitcoin Core Developer Meetup SF, Bicoin Core Developers, April 2018
18. Bay Area Crypto Day 2018, May 2018
19. Annual Stanford Security Forum, Stanford Computer Forum, June 2018
20. ZCon0 Conference, Zcash Foundation, June 2018

21. Novi, Facebook, July 2018
22. Israel Bitcoin Meetup, July 2018
23. Weizmann Institute, July 2018
24. Starkware, July 2018
25. Monero Talk, October 2018
26. NASA Formal Methods 2020, May 2020

### Provisions [Dag+15]

27. Real World Crypto, IACR, January 2016
28. Next Context Conference, Digital Garage Japan, November 2016
29. Papua New Guinea Government Delegation (deputy prime minister, October 2017
30. Speaker Series @ Coinbase, June 2018

### Verifiable Delay Functions [Bon+18; BGB17]

31. Security & Privacy on the blockchain, IEEE, April 2017
32. CESC 2017, Blockchain @ Berkeley, October 2017
33. zk Prodcast, zeroknowledge.fm, August 2018
34. Charles River Crypto Day, March 2019

### Accumulators [BBF19]

35. **CRYPTO, IACR, August 2019**
36. Scaling Bitcoin, October 2018
37. Stanford Blockchain Conference, Stanford Blockchain Center, January 2019
38. Grincon, Grin Foundation, February 2019
39. Conference on Distributed Ledgers, Harvard Center of Mathematical Sciences, February 2019
40. Visa Research Talk, March 2019
41. Bay Area Crypto Day 2019, May 2019

### Zether [Bün+20a]

42. Tsinghua Xi'an blockchain workshop, IIIS Tsinghua University, December 2018
43. ZK Proof workshop, ZKProof, April 2019

### Flyclient [Bün+20c]

44. **IEEE S&P (Oakland), May 2020**
45. Scaling Bitcoin, November 2017

46. SF Bitcoin Developer Meetup, Bicoin Core Developers, April 2019

47. ZCon1 Conference, Zcash Foundation, June 2019

### DARK [BFS20]

48. Probabilistically Checkable and Interactive Proof Systems, Simons Institute, September 2019

49. Bay Area Crypto Day 2019 Fall, November 2019

50. CESC 2017, SF Blockchain week, November 2019

51. Devcon 5, Ethereum Foundation, December 2019

52. Cornell Crypto Group, Cornell University, May 2020

53. CASA Distinguished Lecture, Ruhr Uni Bochum, January 2021

54. VDF Day #4, VDF Alliance, February 2020

### Inner Pairing Products [Bün+21b]

55. Proofs, Consensus, and Decentralizing Society Reunion, Simons Institute, December 2020

### Accumulation Schemes[Bün+20b; Bün+21a]

56. **CRYPTO, IACR, August 2021**

57. zkStudyClub, zeroknowledge.fm, February 2021

58. CMU Crypto Seminar, May 2021

59. Science of Blockchain Conference, August 2022