

# Benedikt Bünz

✉ bb@nyu.edu • 🌐 bue.nz

## Academic

### Courant Institute NYU

*Assistant Professor Computer Science, Tenure Track*  
Research Areas: Applied Cryptography, Blockchains

New York City, New York

Since 2023/9

### Stanford University

*PhD in Computer Science, Advised by Dan Boneh*  
Thesis: Improving the Privacy, Scalability, and Ecological Impact of Blockchains

Stanford, California

2016/9 – 2023/6

### Stanford University

*MS in Computer Science*  
Specializations: Artificial Intelligence and Theoretical CS

Stanford, California

2014/9 – 2016/6

### University of Zurich

*BS in Computer Science, Summa cum laude*  
Bachelor Thesis: Faster Algorithms and Better Payment Rules for Core-Selecting Combinatorial Auctions

Zurich, Switzerland

2011/9 – 2014/8

## Work Experience

### Research Positions

#### Espresso Systems

*Cofounder and Chief Scientist*

San Francisco, California

Since 2021/1

#### Visa Research

*Intern, PhD Summer Intern*

Confidential Smart Contracts

Palo Alto, California

6/17 to 9/17

#### University of Zurich

*Research Internship, Computing BNEs in Combinatorial Auctions*

Advised by Sven Seuken and Ben Lubin

Zurich, Switzerland

Summer '15

#### Stanford University

*Research Assistant, Provisions*

Dan Boneh

Stanford, California

Spring '15

### Teaching Positions

#### New York University

*Instructor, Cryptography of Blockchains*

New York City, New York

Spring '24

#### Stanford University

*Instructor, Cryptocurrencies and Blockchain Technologies (CS 251)*

Co-taught with Dan Boneh

Stanford, California

Fall '20 and '21

#### Stanford University

*Teaching Assistant, Cryptography (CS 255)*

Taught by Dan Boneh

Stanford, California

Winter '16

#### Stanford University

*Teaching Assistant, Bitcoin and Cryptocurrencies (CS 251)*

Taught by Dan Boneh and Joseph Bonneau

Stanford, California

Fall '15

## Awards and Scholarships

<b>VeChain</b> <i>Graduate Fellowship</i> Supporting PhD Studies	<b>Stanford, California</b> 2020/9
<b>Microsoft</b> <i>Research Fellow at Simons Institute</i> Proofs, Consensus and Decentralization workshop	<b>Berkeley, California</b> 2019/9
<b>Studienstiftung des Deutschen Volkes</b> <i>Auslandsstipendium, International studies scholarship</i> 35,000 EUR grant from the German Academic Scholarship Foundation	<b>Bonn, Germany</b> 2014/8
<b>Zühlke Technology Group AG</b> <i>Graduate studies scholarship, zuehlke.com</i> 9,000 CHF	<b>Schlieren, Switzerland</b> 2014/8
<b>University Zurich</b> <i>Semester Price, uzh.com</i> Best 30 thesis per semester	<b>Zurich, Switzerland</b> 2015/4
<b>German Academic Scholarship Foundation</b> 2016/6, Bonn, Germany studienstiftung.de Awarded to top 0.5% of German students	<b>Studienstiftung des Deutschen Volkes</b> 2012/9

## Publications

### Publication Highlights and Summary.....

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

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

[BC24] **Bünz**, B., Chen, J., "Proofs for Deep Thought: Accumulation for large memories and deterministic computations". In: *IACR Cryptol. ePrint Arch.* (2024).

<sup>1</sup><https://web.getmonero.org/resources/moneropedia/bulletproofs.html>

<sup>2</sup><https://www.coindesk.com/business/2019/05/28/jpmorgan-adds-privacy-features-to-ethereum-based-quorum-blockchain/>

<sup>3</sup><https://finance.yahoo.com/news/chia-network-153251783.html>

<sup>4</sup><https://slideslive.com/38911623/ethereum-20-randomness>

<sup>5</sup><https://www.vdfalliance.org/>

[Bün+24] **Bünz**, B., Mishra, P., Nguyen, W., Wang, W., “Accumulation without Homomorphism”. In: *IACR Cryptol. ePrint Arch.* (2024).

[BC23] **Bünz**, B., Chen, B., “ProtoStar: Generic Efficient Accumulation/Folding for Special Sound Protocols”. In: *To appear at ASIACRYPT 2023* (2023).

[Che+23] Chen, B., **Bünz**, B., Boneh, D., Zhang, Z., “HyperPlonk: Plonk with Linear-Time Prover and High-Degree Custom Gates”. In: *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part II*. Ed. by Carmit Hazay and Martijn Stam. Lecture Notes in Computer Science. Springer, 2023.

[Das+23] Das, S., Camacho, P., Xiang, Z., Nieto, J., **Bünz**, B., Ren, L., “Threshold Signatures from Inner Product Argument: Succinct, Weighted, and Multi-threshold”. In: *To appear at CCS 2023* (2023).

[Xio+23] Xiong, A. L., Chen, B., Zhang, Z., **Bünz**, B., Fisch, B., Krell, F., Camacho, P., “VeriZexe: Decentralized Private Computation with Universal Setup”. In: *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*. Ed. by Joseph A. Calandrino and Carmela Troncoso. USENIX Association, 2023.

[BF22] **Bünz**, B., Fisch, B., “Schwartz-Zippel for multilinear polynomials mod N and Lattice-Based Succinct Arguments”. In: *To appear at TCC 2023* (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](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

[BLS22] **Bünz**, B., Lubin, B., Seuken, S., "Designing Core-Selecting Payment Rules: A Computational Search Approach". In: *Inf. Syst. Res.* 4 (2022).

[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](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](http://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
- Crypto 2023 PC Member
- CCS 2021, CCS 2023 PC Member
- AFT 2021, AFT 2023 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

---

<b>E.P. Patent No. EP3665858A4</b> <i>Verification of interactions system and method</i>	<b>Pending</b> <i>Assigned to Visa</i>
<b>U.S. Patent No. US20190164153A1</b> <i>Blockchain system for confidential and anonymous smart contracts</i>	<b>Pending</b> <i>Assigned to Visa and Stanford</i>
<b>U.S. Patent No. US20200252221A1</b> <i>Optimizations for verification of interactions system and method</i>	<b>Pending</b> <i>Assigned to Visa and Stanford</i>