Benedikt Bünz

✉ benedikt@cs.stanford.edu • crypto.stanford.edu/~buenz

Education

Simons Institute — **Berkeley, California**
Microsoft Research Fellow, Proofs, Consensus, and Decentralizing Society — *Fall 2019 – 2019*

Stanford University — **Stanford, California**
PhD in Computer Science, Advised by Dan Boneh — *Since 2016/9*
Interests: Applied Cryptography, Security

Stanford University — **Stanford, California**
MS in Computer Science — *2014/9 – 2016/4*
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

Translucence, Inc. — **Menlo Park, California**
Chief Scientist — *Since 2020/11*

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*
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 Crypto Currencies (CS 251) — *Fall '15*
Taught by Dan Boneh and Joseph Bonneau

University of Zurich — Zurich, Switzerland
Teaching Assistant, Combinatorial Auctions — Spring '14 – 2014
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

Studienstiftung des Deutschen Volkes — Bonn, Germany
German Academic Scholarship Foundation, studienstiftung.de — 2012 – 2016
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. Top 100 security paper by age-normalized citation. [3].
- Verifiable Delay Functions[Bon+18] are already used by the 'green' cryptocurrency Chia[4] and are planned for Ethereum 2.0[5], Filecoin and others. There also exists an industry wide VDF alliance[6] that is funding research on VDF and VDF hardware development. [Bon+18] is a top 100 cryptography paper by age normalized citation count[7].
- 6 papers at top cryptography conferences (CRYPTO, EUROCRYPT, ASIACRYPT, TCC)
- 3 papers at top security conferences (IEEE S&P, CCS)
- 4 papers at top AI and EconCS conferences (AAAI, IJCAI, ICLR, EC)

[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://www.sec.cs.tu-bs.de/~konrieck/topnotch/sec_ntop100.html
[4] https://finance.yahoo.com/news/chia-network-153251783.html
[5] https://slideslive.com/38911623/ethereum-20-randomness
[6] https://www.vdfalliance.org/
[7] https://www.sec.cs.tu-bs.de/~konrieck/topnotch/crypto_ntop100.html

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

[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#:~:text=A%20proof%20of%20solvency%20demonstrates,any%20information%20about%20its%20customers..

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

[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
- Subreviewer Eurocrypt, IndoCrypt, Asiacrypt, Crypto, IEEE S&P, CCS, and others

Interests and Extracuricular Achievements

- Track Running (800m to 5000m): 5 medals in Swiss Relay and Team Championships, 4:08 mile pr
- Bike tour across the US www.crazyguyonabike.com/doc/18076
- Travel
- Current Political Events