Benedikt Bünz

benedikt@cs.stanford.edu • https://crypto.stanford.edu/~buenz

Education

Stanford University — **Stanford, California, USA**
PhD in Computer Science, Advised by Dan Boneh — *2016/9 – 2021*

Interests: Applied Cryptography with focus on Cryptocurrencies

Stanford University — **Stanford, California, USA**
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

Publications

Cryptography and Security

Boneh, D., Bonneau, J., Bünz, B., Fisch, B., (2018). "Verifiable Delay Functions". In: *38th International Cryptology Conference*. URL: https://eprint.iacr.org/2018/601.pdf.

Boneh, D., Bünz, B., Fisch, B., (2018). "Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains". In: *Preprint eprint:2018:1188*. URL: https://eprint.iacr.org/2018/1188.

Bünz, B., Agrawal, S., Zamani, M., Boneh, D., (2018). "Zether: Towards Privacy in a Smart Contract World". In: URL: https://crypto.stanford.edu/~buenz/papers/zether.pdf.

Bünz, B., Bonneau, J., Goldfeder, S., (Jan. 2017). "Proofs-of-delay and randomness beacons in Ethereum". In: *IEEE SECURITY & PRIVACY ON THE BLOCKCHAIN (IEEE S&B)*. URL: http://www.jbonneau.com/doc/BGB17-IEEESB-proof_of_delay_ethereum.pdf.

Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G., (May 2018). "Bulletproofs: Short Proofs for Confidential Transactions and More". In: *39th IEEE Symposium on Security and Privacy (SP)*. URL: https://eprint.iacr.org/2017/1066.pdf.

Bünz, B., Kiffer, L., Luu, L., Zamani, M., (2018). "Flyclient: Super-Light Clients for Cryptocurrencies". In:

Dagher, G. G., Bünz, B., Bonneau, J., Clark, J., Boneh, D., (Oct. 2015). "Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges". In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, pp. 720–731. URL: https://eprint.iacr.org/2015/1008.pdf.

Artificial Intelligence

Selsam, D., Lamm, M., Bünz, B., Liang, P., Moura, L., Dill, D. L., (2018). "Learning a SAT Solver from Single-Bit Supervision". In: *arXiv preprint arXiv:1802.03685*. URL: https://arxiv.org/abs/1802.03685.

Economics and Computation

Bosshard, V., Bünz, B., Lubin, B., Seuken, S., (Aug. 2017). "Computing Bayes-Nash Equilibria in Combinatorial Auctions with Continuous Value and Action Spaces". In: *IJCAI-17*. URL: http://www.ifi.uzh.ch/ce/publications/BNE_Bosshard_et_al_IJCAI_2017.pdf.

Bünz, B., Lubin, B., Seuken, S., (June 2018). "Designing Core-Selecting Payment Rules: A Computational Search Approach". In: *19th ACM Conference on Economics and Computation*. URL: https://ssrn.com/abstract=3178454.

Bünz, B., Seuken, S., Lubin, B., (Feb. 2015). "A Faster Core Constraint Generation Algorithm for Combinatorial Auctions". In: *AAAI 2015*. URL: http://www.ifi.uzh.ch/ce/publications/A_Faster_CCG_Algorithm_Buenz_et_al_AAAI_2015.pdf.

Lubin, B., Bünz, B., Seuken, S., (July 2015). "New Core-Selecting Payment Rules with Better Fairness and Incentive Properties". In: *AMMA 2015*. Extended abstract of working paper. URL: http://www.ifi.uzh.ch/ce/publications/Fairness_and_Incentives.pdf.

Work Experience

Research Positions

Visa Research — **Palo Alto, California, USA**
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, USA**
Research Assistant, Provisions — *Spring '15*
Dan Boneh

Teaching Positions

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

Stanford University — **Stanford, California, USA**
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*
Taught by Sven Seuken

Awards and Scholarships

ZCash Foundation — **Stanford, California, USA**
ZCash Foundation Fellowship, — *2018/9*
Research on Zero-Knowledge Proofs: $40'000

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

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

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

Studienstiftung des Deutschen Volkes — **Bonn, Germany** — *2012 – 2016*
German Academic Scholarship Foundation, studienstiftung.de
Awarded to top 0.5% of German students

Academic Service

Pencil Workshop — **Darmstadt, Germany** — *2019/5*
Program Committee Member

Stanford Blockchain Conference — **Stanford, California, USA** — *2019/1*
Program Committee Chair

Scaling Bitcoin — **Tokyo, Japan** — *2018/10*
Program Committee Member

Scaling Bitcoin — **Stanford, California, USA** — *2017/10*
Program Committee Member

Workshop and Conference Talks

Xi'an Blockchain Workshop — **Xi'an, China** — *2018/12*
Zether, Invited Talk

Scaling Bitcoin — **Tokyo, Japan** — *2018/10*
Accumulators, Peer-reviewed

Zcon0 — **Montreal, Canada** — *2018/6*
A Bulletproof Update, Invited Talk

S & P (Oakland) — **San Francisco, California, USA** — *2018/5*
Bulletproofs, Conference with Proceedings

Scaling Bitcoin — **Stanford, California, USA** — *2017/9*
State of Cryptography, Keynote

Scaling Bitcoin — **Stanford, California, USA** — *2017/9*
Flyclient, Peer Reviewed

IEEE S & B — **Paris, France** — *2017/4*
Randomness Beacons and Delay Functions, Peer Reviewed

CESC — **Berkeley, California, USA** — *2016/10*
Randomness Beacons and Delay Functions, Peer Reviewed

INFORMS Annual Meeting — **Nashville, Tennessee, USA** — *2016/11*
Provisions, Invited

Real World Crypto — **Stanford, California, USA** — *2016/1*
Provisions, Invited

AAAI — **Austin, Texas, USA** — *2015/2*
A Faster CCG Algorithm, Conference with Proceedings

Non-academic Interests

- 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
- Chess