

Education

- **University of Illinois at Urbana-Champaign** Urbana, IL
Advisor: Andrew Miller, PhD in ECE 2018 - Present
 - Focus on cryptocurrencies, decentralized systems, security
- **University of Illinois at Urbana-Champaign** Urbana, IL
Advisor: Andrew Miller, Master of Science in ECE 2016 - 2018
- **University of Illinois at Urbana-Champaign** Urbana, IL
Bachelor of Science in ECE 2012-2016

Experience

- **Graduate Researcher at Decentralized Systems Lab** Urbana
Advisor: Andrew Miller 2016 - Present
 - Decentralized systems security, smart contracts
 - Research work below.
- **Flashbots**
Grant Researcher 2021
 - Worked towards a better auction mechanism for MEV auctions. Completed a literature survey and continue to collaborate on mechanism design for the next iteration of the auction.
- **Truebit**
Researcher 2018 - Present
 - Doing research into securing and designing the Truebit incentive layer and token mechanics. More broad work into cryptoeconomic problems as well as implementation of incentive layer.
 - Working on bringing Truebit to deployment, building their interactive coin offering (ICO) smart contract, working with developers to create the user interface for it.
- **ExoWear**
Software Engineer 2016
 - Start-up in medical technology that provides a Bluetooth device to help monitor physical rehabilitation
 - Worked on developing the core product and managed other engineers
- **Undergraduate Researcher at Depend Research Group** Urbana
Undergraduate Researcher, Advisor: Zbigniew Kalbarczyk 2015-2016
 - Attack testbed that simulates different attacks from web applications to DDoS, remote code execution, SSL vulnerabilities
- **Akuna Capital** Champaign, IL
Software Developer Intern 2015
 - C++ gateways that send buys/sells to exchange and handle book keeping

Research

- **Tokenized Law Review** 2020
S. Bakshi, S. Kim, A. Miller, K. Wetz (Alphabetical)
UCI Law Review - Symposium on The Role of Technology in Academic Publishing A Cross-Disciplinary Discussion 2021
- **PISA: Arbitration Outsourcing for State Channels** 2019
P. McCorry, S. Bakshi, I. Bentov, S. Meiklejohn, A. Miller
ACM AFT 2019
- **Sprites and State Channels: Payments Networks that Go Faster than Lightning** 2019
A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, P. McCorry
Financial Cryptography 2019
- **TxProbe: Discovering Bitcoin's Network Topology Using Orphan Transactions** 2019
S. Delgado-Segura, S. Bakshi, C. Prez-Sol, J. Litton, A. Pachulski, A. Miller, B. Bhattacharjee
Financial Cryptography 2019
- **You Sank My Battleship! A case study to evaluate state channels as a scaling solution for cryptocurrencies** 2019
P. McCorry, C. Buckland, S. Bakshi, K. Wust, A. Miller
Workshop on Trusted Smart Contracts
- **Erays: Reverse Engineering Ethereum's Opaque Smart Contracts** 2018
Y. Zhou, D. Kumar, S. Bakshi, J. Mason, A. Miller, M. Bailey
USENIX 2018
- **Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees** 2018
G. Fanti, S. Bakshi, S. B. Venkatakrishnan, A. Miller, B. Denby, S. Bhargava, P. Viswanath
SIGMETRICS 2018

Projects - Github: <https://github.com/sbaks0820>

- **DyDx MEV** IC3 Bootcamp
K, Solidity 2020
 - Defined the formal semantics of the DyDx exchange protocol in the K framework. The formal model is used with other DeFi models to measure potential miner extractable value.
- **Python-Saucy**
Python 2020
 - An implementation of the UC frame work in Python. The implementation implemented the novel import mechanism and allows protocol fuzz testing and composition.
- **UKK** IC3 Bootcamp
Circom, Solidity 2019
 - An implementation of the Universal Key Knowledge paper by Phil Daian. Worked to implement the SNARK circuit for Bitcoin block header verification in circom. Used for provable miner fairness.

- **Battleship State Channel** IC3 Bootcamp
Solidity, Truffle, Ethereum 2018
 - Project from the IC3 Bootcamp, a Battleship game implemented as a state channel. Uses a combination of the Sprites, Pisa, Perun and L4 state channel construction.
- **microRaiden Off-chain Payment Monitoring** 2018
Solidity, Ethereum, Raiden, Python
 - Implementation of a **privacy-preserving** monitoring protocol for off-chain payment channels on Ethereum
 - **Paper with formal definitions and proofs incoming**
- **hackthiscontract.io** 2017
Solidity, Smart Contract Security
 - Interactive challenges for hacking vulnerable smart contracts and ERC20 tokens
 - Creating games where layered vulnerabilities allows adversaries to violate contract invariants
- **Dandelion++** 2017
Fork of Bitcoin Core and BIP
 - Implementation of Dandelion++ protocol that adds privacy at the p2p level of Bitcoin
 - Article about it on CoinDesk, a BIP-proposal on the Bitcoin Dec mailing list and a paper submission coming soon
- **Python-Bitcoinlib** 2017
Contributor, Bitcoin, Privacy
 - Contribution for segwit support in popular Python Bitcoin library managed by Peter Todd
- **Fair Lottery Smart Contract** 2016
Serpent Programming Language, Ethereum
 - Smart contract that implements a cryptographically fair lottery with a python simulator
- **Echo Dot Permissions Model** 2016
Java, Python Flask, AWS, Alexa Skills
 - Interacts with Alexa Skills and Microsoft Cognitive API to provide access control based on speaker recognition
- **Attack Testbed** 2015
Python, JavaScript, Docker
 - Docker testbed that allows easy creation, simulation, monitoring and replaying of attacks ranging from the application layer down to the network layer
 - Abstract paper: "Security Testbed: Scalable Infrastructure for Interactive Attack Replay and Testing of Security Monitoring Tools"
- **Galapagos** 2015
C, x86 assembly
 - Light Linux-based operation system that runs on x86 assembly with a virtual memory support, scheduling, system calls, multiple terminals, drivers
- **5-Stage Pipelined Processor** 2016
Verilog
 - Pipeline processor with branch prediction, multi-layered LRU caches, leap-frogging
- **FPGA Brick Breaker** 2015
System Verilog, C
 - FPGA brick breaker with verilog vga monitor, keyboard driver support