On my journey to join theclub of people who possess a reasonable understanding of ZKP cryptography, I stumbled upon many invaluable resources that provided to be very helpful. The problem was that they were rather scattered on the web. The awesome ZKP repo is indeed awesome but a bit verbose and lacks videos and podcasts.

The goal of this post is to serve as an entry point for anyone interested to make their baby steps towards understanding the core technical layers of zero-knowledge-whatever. It is important to note that this is definitely not an exhaustive list, but rather a set of supportive resources for ZKPs that have a connection to the blockchain ecosystem.

Legend

- ZKP = Zero-Knowledge Proof
- zkSN

ARK = Zero-Knowledge Succinct Non-Interactive ARgument of Knowledge

- zkST

ARK = Zero-Knowledge Scalable Transparent ARgument of Knowledge

- AZTEC = Anonymous Zero-knowledge Transactions with Efficient Communication

Induction

- [Deck] Elena Nadolinski: Demystifying Zero-Knowledge Proofs
- [Article] Matthew Green: An illustrated primer
- [Podcast] Zero Knowledge FM: Intro to Zero-Knowledge Proofs with Anna Rose & Fredrik Harrysson
- [Video] What Are Zero-Knowledge Proofs
- [Video] Elad Verbin: Zero-Knowledge Proofs and Their Future Applications at Web3 Summit 2018
- [StackExchange] Comparison between SNARKs, STARKs and Bulletproofs

zkSNARKs

- [Article Series] Vitalik Buterin: zkSNARKs Under the Hood
- [Article] Zcash: What are zkSNARKs?
- [Podcast] Zero Knowledge FM: Intro to zkSNARKs with Howard Wu
- [Video] Howard Wu: Rise of the SNARKs

zkSTARKs

- [Video] Eli Ben Sasson: Introduction of zkSTARKs at Technion Cyber and Computer Security Summer School
- [Deck] State of the STARK at Devcon4
- [Article Series] By Vitalik Buterin

Bulletproofs

- [Podcast] Zero Knowledge FM: Benedikt Bünz on Bulletproofs and Verifiable Delay Functions
- [Video] Bulletproofs: Short Proofs for Confidential Transactions and More
- [Video] Benedikt Bünz at SF Bitcoin Devs

AZTEC

- [Article] Zachary Williamson: A dive into the AZTEC protocol
- [Podcast] The Smartest Contract: Confidential transactions on Ethereum via range proof

MimbleWimble

- [Video] Jackson Palmer: What is MimbleWimble
- [Video] Andreas Antonopoulos: Bitcoin Q&A: MimbleWimble and Schnorr signatures

- [Article] Conor O'Higgins: MimbleWimble explained like you're 12

Papers

- Zerocash: Decentralized Anonymous Payments from Bitcoin
- Scalable, transparent, and post-quantum secure computational integrity
- Bulletproofs: Short Proofs for Confidential Transactions and More
- The AZTEC Protocol
- MimbleWimble

Hope this helps! Open to additions and other suggestions.