Privacy Pass+BBS

Watson Ladd, Michele Orrù, many others

In the beginning

We wanted more

- Rate limits
- Selective disclosure
- Issuer blindness
- Longer term pseudonyms
- ....

Our solution

- Boneh-Boyen-Shacham + blind issuance + linear proofs
- Selective disclosure + rate limiting
- Cost: One pairing product + Camenisch Stadler proof
- Issuer blindness: confident we can get it with a bit more
- One token, many uses (but some corners to consider)

Next steps and questions for discussion

- Write draft
- Better code + measurements
- Some thinking through the theory
- Are people interested in this work?
- What additional things do we need?
- Happy to go into more details!