Halo2 Learning Group

0xPARC, ECC, PSE, Scroll

Today

- Learning group logistics
- Program structure/schedule
- Participant & staff introductions
- Intro to PLONK + Halo2

Logistics

- Communication is on Discord, with a few email announcements
  - Discord is home of async discussion as well
  - Channel overview
  - Turn on notifications and check regularly!
- Resources are in Notion
- Add the Google Calendar
- Most programming is 9-11AM PT weekdays, unless otherwise noted
- Sessions will recorded and uploaded
  - We will post some online publicly, in the style of learn.0xparc.org
- You'll get the most out of this if you can spend 5-10hr/wk outside of sync sessions

Program Content

- Understanding and building user-facing applications with Halo2 and PLONKish proving systems
  - Circuits
  - Toolstack
  - Developer tools
- Theory - not a primary focus, but we'll have some resources available
- This is an experimental program!
  - "Learning group" vs. class
- https://learn.0xparc.org and Notion homespace have useful links and collections

Structure / Schedule

- Weeks 1 + 2: Structured(ish) workshops
- Weeks 3 + 4: Hands-on building a project + guest talks from ZK/Halo2 ecosystem speakers
    - Everyone needs to build something!
- Final demos: Friday 7/8 9AM PT (Put this in your calendar)

Week 1

- Monday: Intro to PLONK/Halo2
- Tuesday: Intro to Halo2 API: Building Fibonacci Circuit
- Wednesday: Math Building Blocks (optional)
- Thursday: Basic Halo2 Gadgets
- Friday: Office Hours (optional)

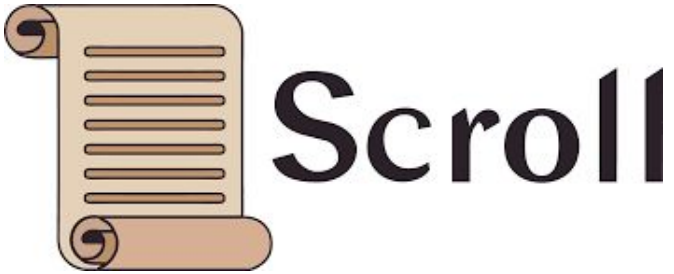
Week 2

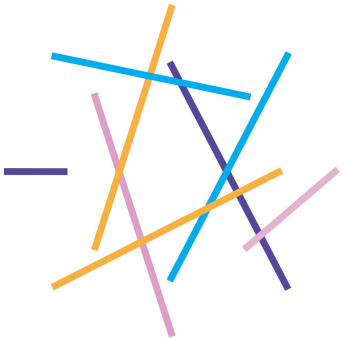
- Monday: Lightning talks #1
  - All participants to give a 3m presentation on some ZK-related topic!
- Tuesday: Circuit exercises, devtooling, test env
- Wednesday: How PLONK works / UltraPLONK deep dive (optional)
- Thursday: Project ideation / matching session
- Friday: Review circuit exercises

Norms

- Wide range of backgrounds, and areas of expertise: crypto theory, engineering, dapp engineering, …
- Sessions may move fast, and so you may find post-session review and questions important. **No question is too basic!**
    - Ask anything in Discord, and if you can, offer up your own answers to others' questions as well.
- We're here to learn from you too!

About the H2LG contributors





Intros

- Staff + Participants: (Briefly) what you work on in ZK, why you're interested in Halo2
- Observers: Post an intro in Discord!

Thesis

vitalik.eth
@VitalikButerin

Replying to @tarunchitra

I expect ZK-SNARKs to be a significant revolution as they permeate the mainstream world over the next 10-20 years.

5:40 PM · Sep 1, 2021 · Twitter Web App

537 Retweets **198** Quote Tweets **2,732** Likes

Thesis

- ZK crypto (specifically SNARKs, STARKs, etc. - ZKPs for arbitrary computation) is more important and general than people think it is

- ZK crypto is easier to use than people realize it is

- PLONKish proving systems are likely to be the future of ZK-enabled applications