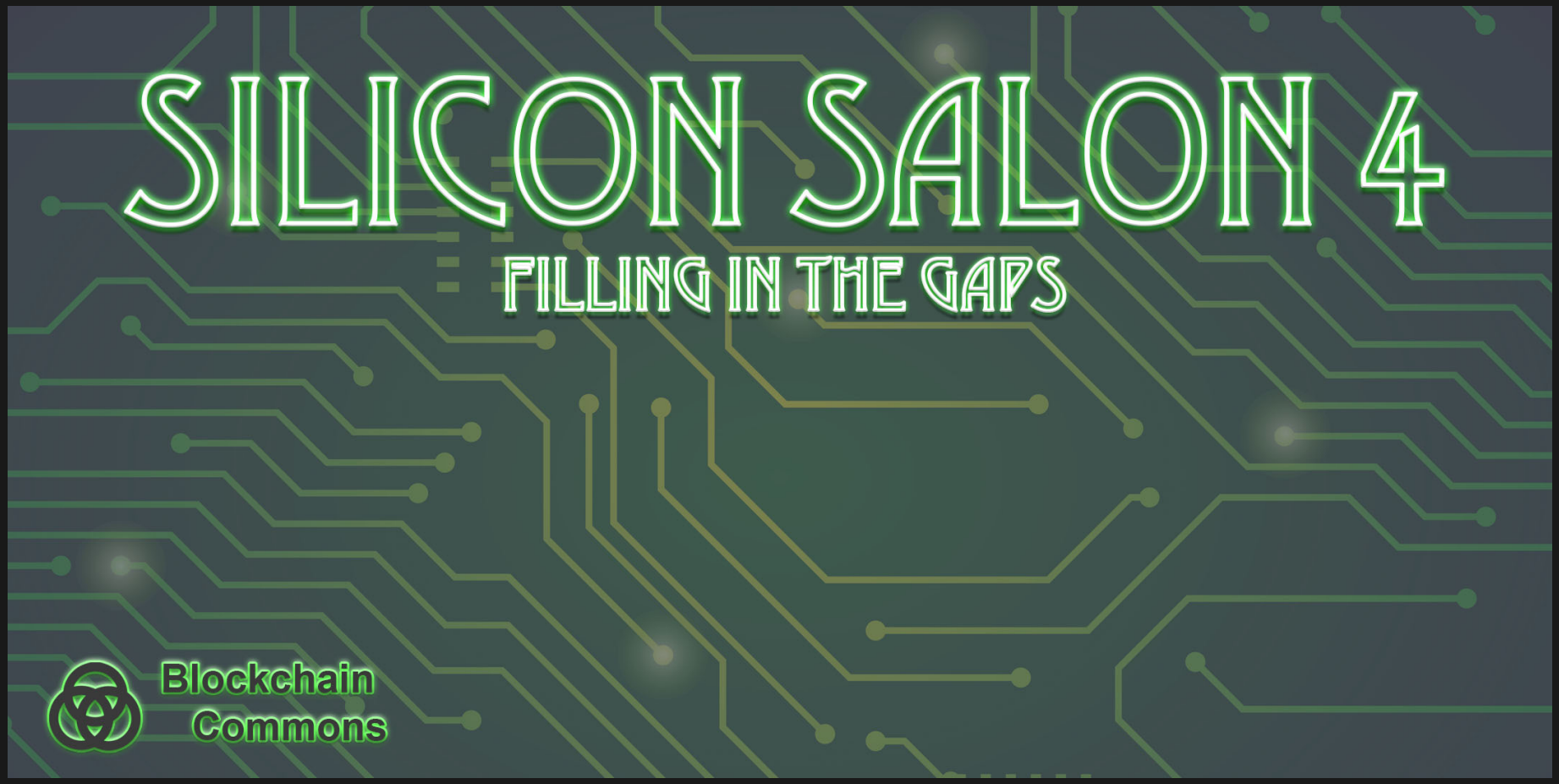


#SiliconSalon IV 2023-05-03

This is collaborative session

You can follow these slides at:

https://hackmd.io/@bc-silicon-salon/BkoVLgkNn#/

Collaborative notes at:

https://hackmd.io/1u3aWfCjQ_aqXc36rdADWQ?edit

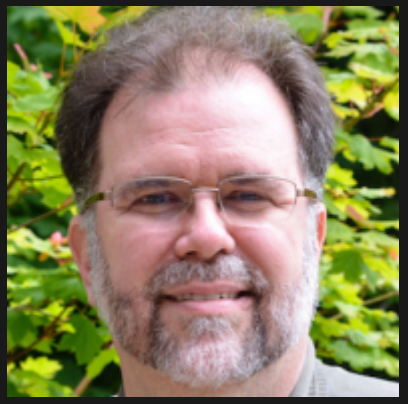
Please join us on a laptop or smartphone!

Live transcription generously contributed by Bryan Bishop!

What is Blockchain Commons?

- We are a community interested in self-sovereign control of digital assets.
- We bring together stakeholders to collaboratively develop interoperable infrastructure.
- We design decentralized solutions where everyone wins.
- We are a neutral “not-for-profit” that enables people to control their own digital destiny.

Who am I?



Christopher Allen (@ChristopherA)

Principal Architect & Executive Director

What is a Silicon Salon?

- Bridge wallet requirements & semiconductor development, academic research & real-world practice.
    - ***This is what we're doing today in this salon!***
- Use what we learn to collaboratively engineer interoperable specifications.
- Evangelize these solutions to the ecosystem.
- Support our partners with reference code and test suites so that they can develop their own implementations.

Who are you?

- Semiconductor designers
  - Bunnie Studios, CrossBar/Cramium, Tropic Square
- Wallet hardware manufacturers
  - Foundation, Proxy, Validating Lightning Signer
- Blockchain & Web3 ecosystem members
  - Bitmark, Chia, Unchained Capital
- Advocacy organizations
  - Human Rights Foundation, Rebooting Web of Trust
- Academics, cryptographic engineers, protocol designers, and cryptographers

Last Event

www.SiliconSalon.info/salon3

Multi-Party Computation and More

- What are the current innovations in the industry?
- How can we trust the transitors?
- Our first pure cryptography on silicon presentation!

The challenges we're exploring today...

Filling in the Gaps!

The Process

- SCAN: Multiple presentations on these topics, with limited Q&A
  - *(~ 1 to 1-1/2 hour then a brief break)*
- FOCUS: Facilitated Q&A on Open Hardware
- ACT: Decide on next steps for collaboration
  - *(~15 minutes)*

Collaborative Notes at:

https://hackmd.io/fqvhrHMWTYee_X5o-_VUkQ?edit

Chatham House Rules Apply

- *“participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s) … may be revealed.”*
- We are recording the presentations for YouTube
- We will not be sharing the Q&A, only recording to produce an anonymized summary
- Summary will include quotes, but not names
- You can request anything you said be removed from the final summary

Presentations

- **Anti-Exfil: Preventing Key Exfiltration Through Signature Nonce Data**
  - *Andrew Poelstra, Blockstream*
- **Scalar and Vector Draft Biginteger instructions for the Power ISA**
  - *Luke Kenneth Casson Leighton & David Calderwood*
- **Pitfalls and Approaches to Open Source Security Semiconductor**
  - *Dr. Mark Davis, Cramium*

- ***Andrew Poelstra*** is the Director of Blockstream Research, a team of cryptographers, Bitcoin developers, and network engineers that has extensive experience working in depth on the Bitcoin protocol. Andrew has helped to invent several privacy and scalability technologies in the Bitcoin space, including Confidential Transactions, Taproot, Miniscript, MuSig, and Scriptless Scripts.

- ***Luke Leighton*** is an Ethical Technology Specialist, lead on Libre-SOC, and the Technical Director and Founder of RED Semiconductor Ltd.
- ***David Calderwood*** is a high-tech team builder with career-long engineering expertise in telecommunications, semiconductors, and computing. He is a Chartered Engineer and FIET and Founder of RED Semiconductor Ltd.
- ***RED Semiconductor Ltd*** is commercialising the Libre-SOC Vector instruction set designed for ground-breaking computational performance and reduced power consumption.

- ***Dr. Mark Davis*** is an entrepreneur and technologist in the field of semiconductors, communications, signal processing, and system design. He was a founder of semiconductor company VIA Telecom (威睿电通) and of the ACJA (www.gutma.org/acja) and today is the president of Crossbar, working on ReRAM memory. Cramium is a new subsidiary of Crossbar.

Break

Get up and stretch! Have a snack! Take a break!

We'll be back in 5 minutes for a discussion of Open Hardware

Open Hardware Presentation Discussions

- What IP Rights protect hardware?
  - Do we just focus on copyright & hope it turns out OK?
- What's the purpose of opening up Hardware?
  - What do we want out of it?
  - What are our goals?

Cramium's Open Approach

- Any thoughts on Cramium/Bunnie Studios/Kosagi approach?
    - Too pragmatic or not pragmatic enough?
    - Are people really going to run and evaluate the RTL on FPGA prototypes?
    - What are the financial incentive for multiple people to give meaningful review?
    - What are the processes to solicit and get feedback from community?
- Current software CVE & bounty policies and best practices don't work for hardware * White hat give notice? (90 days EU reg?)
- What should be the best practices today for our community?

More Thoughts on Open Silicon

- See: https://tinyurl.com/musings-silicon
- Open Silicon aligns with Kerckhoffs' Principle
  - A cryptographic system's security should rely solely on the secrecy of the key, not on the obscurity of the algorithm or its implementation.
- It also creates trust
  - We (mostly) know foundation is secure.
- But ...

Benefits Must Be Concrete!

How about ...

- More scrutiny of design, software layers
- Size & structure constraints
- Risk mitigation vs. proprietary designs
- Rapid exchange of ideas & development
- Trust & credibility
- Reduced vendor lock-in
- Shared costs
- *Are these enough, especially for manufacturers? What are we missing?*

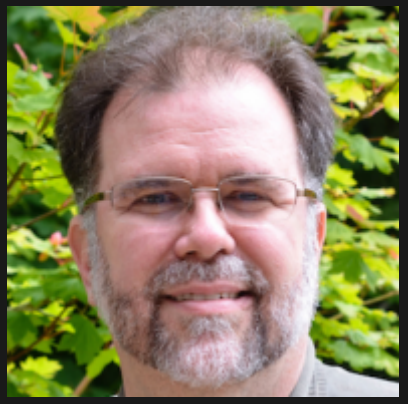
More Thoughts on Challenges

- How do we balance openness & security?
- How do we coordinate a diverse community?
- How do we ensure transitors match RTL design?
- How do we overcome resistance to change?
- How do we make initial investment?
- *We feel that collaboration is key!*
    - *Hence the Silicon Salons*

Next Steps

- Collaboration channels for futher discussion
  - Synchronous: Private Signal group
  - Asynchronous: Github discussion area
- Next Silicon Salon?
  - Late July?
  - Make a Proposal! https://www.siliconsalon.info/proposals/
- Do you like what we are doing here today?
  - Become a ongoing sponsor of Blockchain Commons via GitHub.

www.BlockchainCommons.com



Christopher Allen (@ChristopherA)