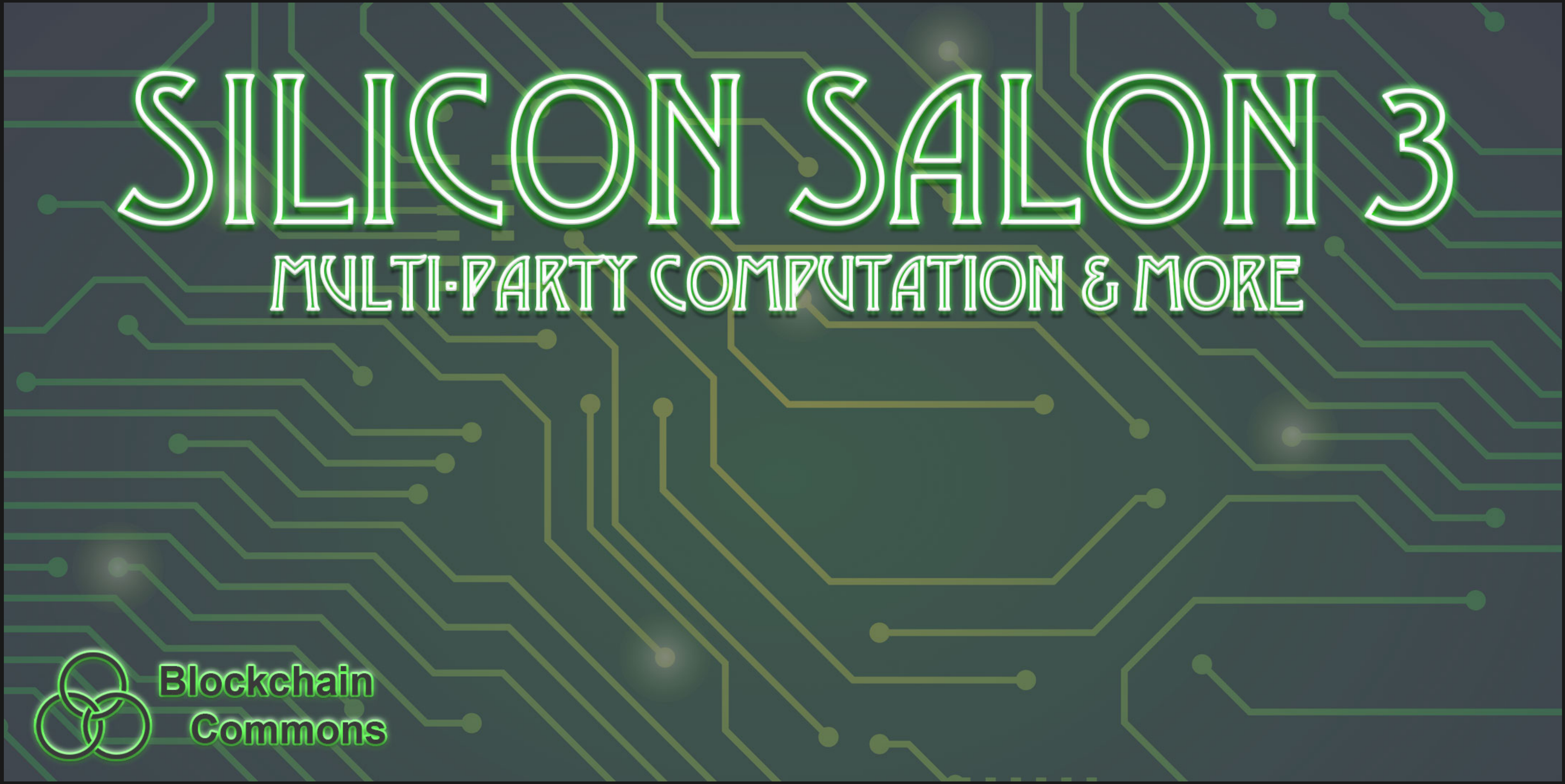

#SiliconSalon III 2023-01-18

This is collaborative session

You can follow these slides at:

https://hackmd.io/mG1lQ2mkTKSqoz4ELYuXHg?view/

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?

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/salon2

Secure Boot, Supply-Chain Security, and Firmware Upgrades

- How do we boot securely?
- How do we ensure firmware is secure?
- How do we update firmware?
- How do we ensure the supply chain isn’t at risk?

The challenges we're exploring today...

Silicon-logic-based cryptographic functionality

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
- ACT: Decide on next steps for collaboration
  - *(~15 minutes)*

Collaborative Notes at:

https://hackmd.io/1u3aWfCjQ_aqXc36rdADWQ?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

- **Silicon & MPC**
    - *Sung-Hyun Jo, Crossbar/Cramium*
- **Toward a More Open Secure Element** Chip
    - *Andrew "bunnie" Huang, Bunnie Studios*
- **A Fast Large-Integer Extended GCD Algorithm and Hardware Design for Verifiable Delay Functions and Modular Inversion**
    - *Kavya Sreedhar, Stanford*

- ***Dr. Sung Hyun Jo*** is the CTO and co-founder of Crossbar. His key expert area includes emerging nonvolatile memory technologies, neuromorphic systems and hardware security. He received various technical awards including Human-Tech Award from Samsung, and the MRS Award for ReRAM research. He holds over 100 patents and over 40 technical publications with 10,000+ citations. Dr. Jo earned his Ph.D. from the University of Michigan.

- ***Andrew “bunnie” Huang*** is an American researcher and hacker, who holds a Ph.D in electrical engineering from MIT and is the author of the freely available 2003 book Hacking the Xbox: An Introduction to Reverse Engineering. He is also a resident advisor and mentor to hardware startups at HAX, an early stage hardware accelerator and venture capital firm.

- ***Kavya Sreedhar*** is an electrical engineering PhD student at Stanford advised by Mark Horowitz. Her current research explores how to efficiently accelerate the extended GCD computation for verifiable delay functions and modular inversion in cryptography. She previously worked with the Agile Hardware (AHA) Project in developing Lake, a parameterizable memory generator that can be configured at runtime to support different image processing and machine learning applications.

Discussion

Next Steps

- Collaboration channels for futher discussion
  - Synchronous: Private Signal group
  - Asynchronous: Github discussion area
- Next Silicon Salon?
  - April 26th (Wednesday, 5pm PT)
- Do you like what we are doing here today?
  - Become a ongoing sponsor of Blockchain Commons via GitHub.

www.BlockchainCommons.com

Christopher Allen (@ChristopherA)