

SILICON SALON 2

SUPPLY-CHAIN SECURITY & FIRMWARE UPGRADES

PRECURSOR →



#bc-silicon-salon 2022-09-14

This is collaborative session

You can follow these slides at:

<https://hackmd.io/9v0ABBXoTyyqzUcF3vDEsg?view/>

Collaborative Notes at:

https://hackmd.io/4UynsiS_SBO9EIDGuZ2AHw?edit

Please join us on a laptop or smartphone!



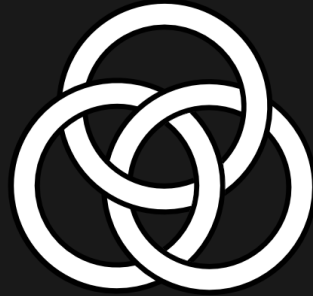
What is Blockchain Commons?

- We bring together blockchain & Web3 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?

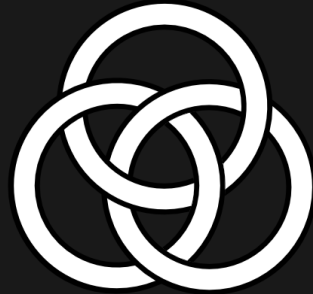
Who are you?

- Semiconductor designers
 - Bunnie Studios, CrossBar/Cramium, Tropic Square
- Wallet hardware manufacturers
 - Foundation Devices, Proxy, Validating Lightning Signer
- Blockchain & Web3 ecosystem members
 - Bitmark, Unchained Capital
- Advocacy organizations
 - Blockchain Bird, Human Rights Foundation
- Cryptographic engineers & protocol designers & cryptographers

Last Event

www.SiliconSalon.com

- Topic: Requirements for Secure Hardware
 - Pain Points
 - Architecture
 - Boot, Firmware & Supply Chain
 - Cryptographic primitives, protocols & acceleration
 - Threats & Countermeasures
 - Edge Topics
 - Building a secure infrastructure ecosystem
- 5 Presentations
 - Blockchain Commons, CrossBar, Proxy, Libre-SOC, Tropic Square
 - Videos, Presentations, and Transcripts
- Key Quotes



The hardware wallet challenges we're exploring today...

- 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 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/4UynsiS_SBO9EIDGuZ2AHw?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 will have an opportunity to request anything you said be removed from the final summary

Presentations

- Bunny Studios
- Crossbar/Cramium
- Proxy
- Foundation Devices
- Validated Lightning Signer

Boot Questions

How do we design bootloader securely
but with flexibility?

Firmware Questions

How do we ensure firmware is secure? How do we update it?

- Auditability, verifiability & public audits of code & secret management
 - manufacturer vs oem requirements?
 - What is "certified" vs "open"?
 - How can we ensure security given black box code?
Deterministic builds?
- Where are multiple security domains a solution?
 - With architectures of multiple chips, what are acceptable limits for updating different chips?
- How to remove compromised keys with updates?
 - Threshold signatures for firmware keys?

Supply Chain Questions

How do we ensure the supply chain isn't at risk?

- Hardware supply chain authentication
 - How far back does supply chain authentication need to go?
 - Back to chipmaker? Verify mask? How
- New forms of authentication?
 - particularly as major manufacturers move away from passwords
 - CPACE, OPAQUE rather than PINs?
- Software supply chain
 - Verification of dependencies

The Bigger Picture

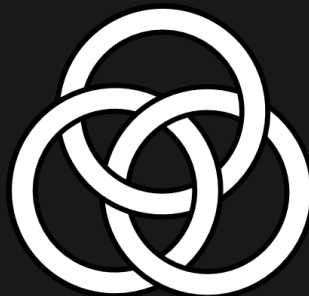
- Who are we missing from this discussion?
- What are our priorities for further discussion, requirements, new specifications, APIs, reference code?
 - Any “low-hanging fruit” that need investigation collectively?
- Talent: We need more cryptographers, code review, hardware designers
 - Hiring/job board?
 - Cryptographers as a shared resource?
 - Peer security code reviews?
- Is there more things that a neutral third-party like Blockchain Commons should be doing?

Next Steps

- Collaboration channels for further discussion
 - Synchronous: [Private Signal group](#)
 - Asynchronous: [Github discussion area](#)
- Next Silicon Salon?
 - November? January?
- Do you like what we are doing here today?
 - Become an ongoing [sponsor](#) of Blockchain Commons via GitHub.



Christopher Allen (@ChristopherA)



www.BlockchainCommons.com