#bc-silicon-salon 2022-06-01

This is collaborative session

You can follow these slides at:

https://hackmd.io/@bc-silicon-salon/rkxbd6rFw9?view#/

Collaborative Notes at:

https://hackmd.io/S7raK1MdSWWciO_Ctm_uhw?edit

Please join us on a laptop or smartphone!

Who am I?

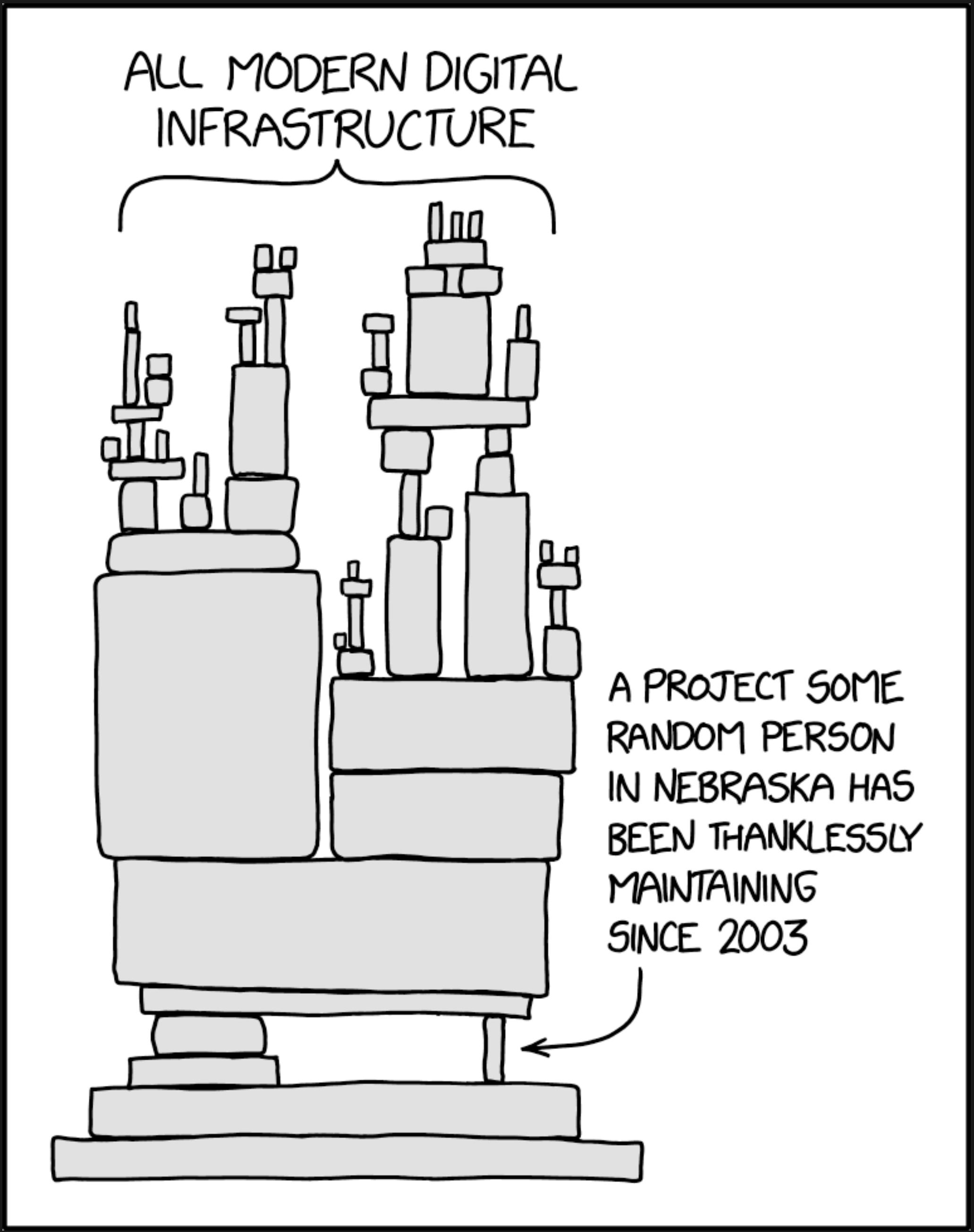
Christopher Allen (@ChristopherA)

- '90s: **Architect**: *RSAREF* & *SSLREF*; **Consultant:** Amix, Xanadu, PGP, RSA, Digicash; **Editor & Co-Author:** *TLS 1.0*
- '00s: **CTO:** Certicom; **Adjuct Professor:** BGI Sustainable MBA
- '10s **VP:** Blackphone; **Founder:** #RebootingWebOfTrust; **Author:** *10 Principles of Self-Sovereign Identity*; **Principal Architect:** Blockstream
- '20s **Co-author:** *W3C Decentralized Identifiers (DIDs)*; **Principal Architect:** Blockchain Commons

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.

The problem we’re solving…


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

What do we do?

- We work with blockchain & Web3 communities to identify problems & assess needs.
  - **This is what we’re doing today in this salon!**
- We use what we learn to collaboratively engineer interoperable specifications.
- We evangelize these solutions to the ecosystem.
- We support our partners with reference code and test suites so that they can develop their own implementations.

I’ve done this before:

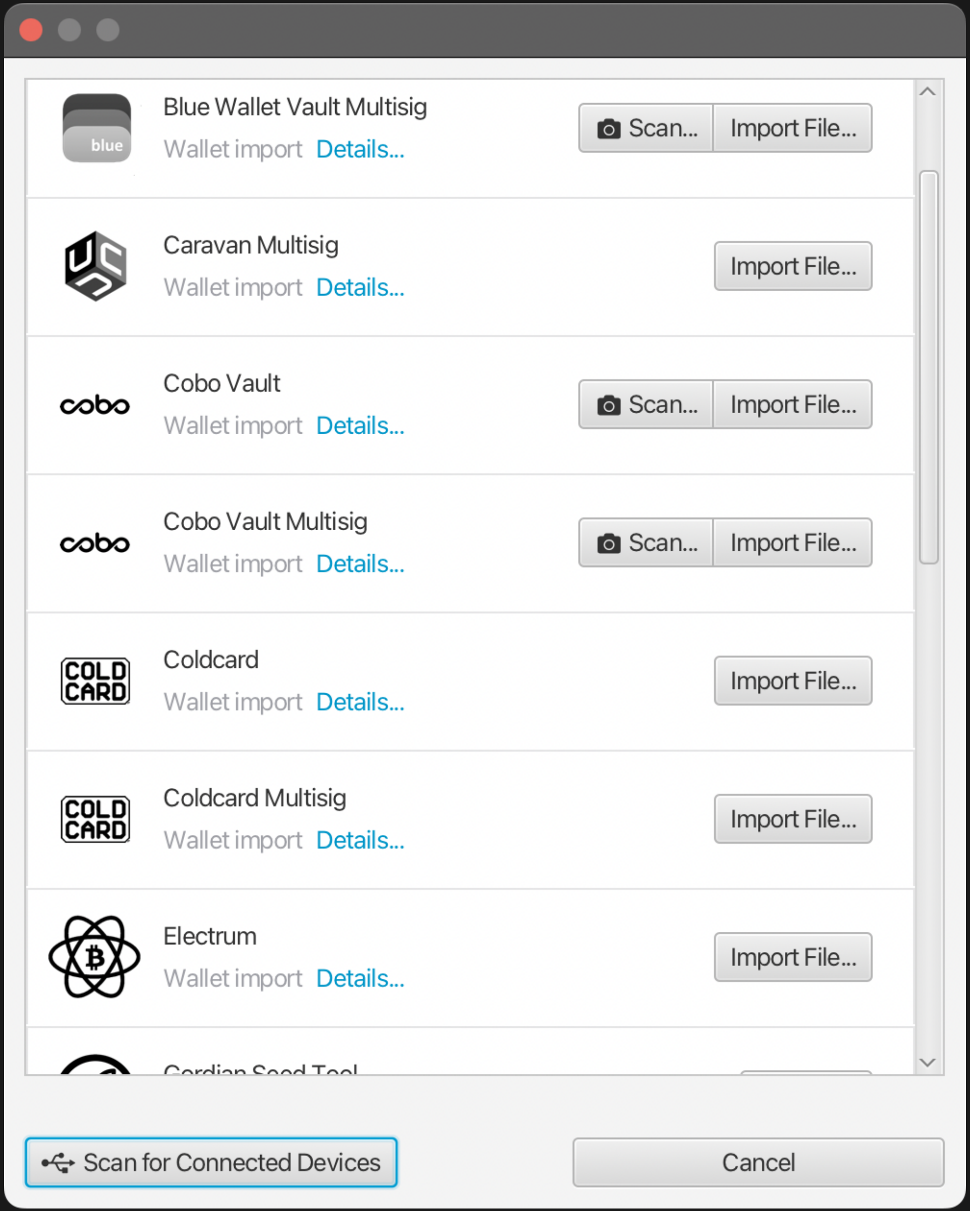
- RSAREF, SSL, TLS
- OAuth, FIDO
- DID, VC
- Smart Custody, Airgap URs & QRs, etc.

Who are you?

- Silicon designers
  - CrossBar, Tropic Square, Supranational
- Wallet hardware manufacturers
  - Foundation Devices, Proxy
- Blockchain & Web3 ecosystem members
  - Bitmark, Unchained Capital
- Advocacy organizations
  - Blockchain Bird, Human Rights Foundation
- Cryptographic engineers & cryptographers

Our problem:

- Leveraging secrets held on silicon chips as a “root of trust” is desirable
- Unfortunately…
    - Existing chips don’t support modern cryptography.
    - Standards orgs (IETF, W3C, etc.) are rejecting the needs of the cryptocurrency ecosystem.
    - Capital costs & lead time for chips are high.
    - Inefficient IP licensing creates friction for developers.
    - Current financial incentives fail to create robust, secure infrastructure.
    - There’s the “NASCAR” problem …



Blue Wallet Vault Multisig
Wallet import Details...

Caravan Multisig
Wallet import Details...

Cobo Vault
Wallet import Details...

Cobo Vault Multisig
Wallet import Details...

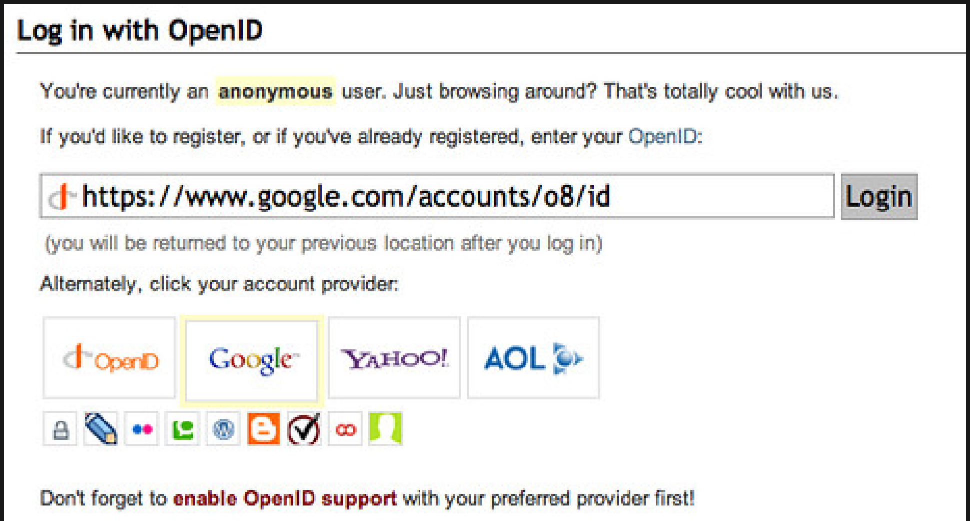
Coldcard
Wallet import Details...

Coldcard Multisig
Wallet import Details...

Electrum
Wallet import Details...

Gordian Seed Tool

The NASCAR problem



Log in with OpenID

You're currently an **anonymous** user. Just browsing around? That's totally cool with us.

If you'd like to register, or if you've already registered, enter your OpenID:

https://www.google.com/accounts/o8/id

(you will be returned to your previous location after you log in)

Alternately, click your account provider:

Don't forget to **enable OpenID support** with your preferred provider first!

We've seen this before:

The Answer

- Follow the process of identification, assessment, collaboration, engineering, evangelization, and support.

We must:

- Work together to define use cases & requirements for new silicon chips.
- Identify essential features for implementing new cryptography securely in silicon logic.
- Create an ecosystem roadmap to support continued investment in secure infrastructure.
- Specify interoperable and future-proof functionality.
- Eliminate privileged points within the ecosystem.
    - Limit ability to subvert the shared protocols.

The Process

- SCAN: Multiple presentations on these topics, with limited Q&A
  - *(~ 1 hour then a brief break)*
- FOCUS: Facilitated Q&A on 6 open topics
  - *(~ 15 minutes each)*
- ACT: Decide on next steps for collaboration
  - *(~15 minutes)*

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

- CrossBar
- Proxy
- Tropic Square
- Libre-SOC
- Supranational

Who am I?

Bryan Bishop (@kanzure)

- Software development background, contractor
- Bitcoin Core contributor, Blockchain Commons sponsor
- previously:
    - LedgerX (now FTX US Derivatives)
    - CTO/co-founder/director @ Custodia Bank (prev. Avanti Bank & Trust)
- Creator of Webcash.org, a cryptocurrency without a blockchain
- Will be taking high-fidelity notes today: https://hackmd.io/@bc-silicon-salon/Byr4vaXOc

Topics

1. Pain points
2. Architectures
3. Boot, firmware & supply chain
4. Cryptographic primitives, protocols & acceleration
5. Threats & countermeasures
6. Edge topics
7. Building a secure infrastructure ecosystem

Pain Points

- Semiconductor support is often limited to SEs
- Lack of secp256k1 (and negative sentiment)
- IP restrictions, patents & NDAs
    - Devkits, lack of which is made worse by NDAs
- NASCAR problem (ecosystem friction)
- One-off cryptography & wallet APIs
- Future proofing as technology evolves & co-existence with legacy
- No one has all the expertise necessary in-house
- Lack of available cryptographer talent (and incentives in academia)
- Market size, government support (and limits)
    - Support for continued investment in secure infrastructure

Pain Point Questions

(15 minutes)

- Any missing pain points?
- Disagree about any?

Architectures

"Establishing next-generation ***roots of trust****"*

- SE only
- Secure key stores
- Accelerator only
- SE(x2?) & MCU
- HSMs & dedicated chips:
    - Titan (Android), Pluton (Windows), T1/T2 (Apple)
    - Java SmartCard
- Secure-on-chip solutions
    - Tee, SGX, TrustZone, vSGX
- MPC & Collaborative Key Generation

Architecture Questions

- Are we missing any important architectures?
- Trusted input/output?
- Integration (and risks) in larger systems?
- What are your perspectives? Where is the market heading?

Boot, Firmware & Supply Chain

- Bootloader: programable, multi-stage
    - Firmware signing & on-chip verification
- Chip maker firmware vs OEM firmware vs user code (SE? MCU? both?)
- Supply chain authentication
- Auditability, verifiability, & public audits of code & secret management

Boot, Firmware & Supply Chain Questions

- Bootloader pain points?
- Can OEM/wallet maker replace root of trust with their own? Self-sovereign devices?
- Where are multiple security domains a solution?
    - “certified” and “open”?
- How far back does supply chain authentication need to go?
- With architectures of multiple chips, what are acceptable limits for updating different chips?
- Pro & cons of MicroPython vs. bare metal code (Rust, etc.)

Cryptographic Primitives

- New hashes, MACs, Key Derivation
    - Blake3, SHA3, Poly1305, BIP32
- Symmetric Encryption
    - AES-512 vs ChaCha (x, 12, 20)
- New curves
    - NIST P-384 (DH, ECDSA, secp384r1)
        - *Soon to be mandated by US-DHS*
    - secp256k1 (DH, ECDSA & Schnorr)
    - IETF (25519, ed25519, x25519)
    - ristretto255 & decalf448
    - BLS12-381
- ZK-friendly
    - Plonk & Halo
- Quantum-attack resistant
    - *Emerging NIST requirements*

Cryptographic Primitives Questions

- Are we missing any cryptographic primitives that should be implemented in silicon
    - Spectrum: how much in RTL vs microcode vs interpreter
- What primitives are challenging for your current hardware?
- How important are NIST and other government standards?
- How important is resistance to quantum computing attacks, to you, today?

Cryptographic Protocols

- Signature Systems
    - Not just signing, but aggregation and revocation
- Certs, Verifiable Credentials and DIDs
    - Browser OpenOAuth, JWTs, DIDComm, Keri
    - Privacy (including BBS+ signatures)
- Multiparty Signature Schemes
    - Schnorr Aggregated: MuSig2, MuSigDN
    - Schnorr Threshold: FROST, TOAST
    - Adaptor Signatures: ECDSA, Schnorr
    - Various MPC protocols…
- Authentication & Key Proofs
    - PAKE, OPAQUE
- Transport
    - IETF TLS, Signal, Noise, IETF MLS
- Cryptocurrencies
    - In particular Smart Signature scripts

Cryptography Protocol Questions

- We can’t support all protocols in dedicated silicon, but what parts are critical for you?
- Is it security or performance that drives your choices?
- How do we do secure hand-off between chips & devices with different capabilities?
    - supporting secure state machines

Crypto Acceleration

- Finite field arithmetic
- ECC multiply/add
- Zero-knowledge proofs, rangeproofs, bulletproofs, SNARKs, etc.
    - Multi-exponentiation
    - Fast Fourier Transforms
- Secret Sharing
    - SSS - Shamir's Secret Sharing
    - VSS - Verifiable Secret Sharing
    - PVSS - Publicly Verifiable Secret Sharing

Crypto Acceleration Questions

- What other functions need hardware acceleration?
    - Which are important to you ***NOW***.
- What performance requirements do you have now?
    - Any benchmarks?
- When accelerating new cryptography (FROST, MPC, etc.), what are the real requirements for silicon protection of secrets?
    - Storage of firmware, state, nonces, etc.
- What additional use cases could be enabled by hardware acceleration?

Threats & Countermeasures

- Supply chain security
- Secure input and output
- Memory privacy, robustness, longevity
- Side-channel resistance
- Chip microcode vs RTL in CMOS for crypto algorithms
- Physical countermeasures
    - **Tamper evident:** some indication of tampering whether successful or not
    - **Tamper resistant:** some resistance to tampering attempts
    - **Tamper-proof:** impossible case?

Threats & Countermeasure Questions

- What are realistic threats?
- Best-practices & countermeastures to address these threats?
- What are your worries about side-channels?
- Any evolving threats that we've not worried about before?
- What attacks are the most critical for silicon chips protect against?
- Are physical countermeasures important, and why?
    - What are your requirements for secure input & output?
    - Is a MCU+SE where the MCU has limited countermeasures just as bad as no SE at all?
- Other "systemic" threats?

Edge Topics

- Use cases, markets, and market size
    - E2E, IoT, oracles, sophisticated smart contracts, HSMs, server key management
- Openness: IP licensing, NDAs, etc.
    - What does Open Development mean for chips?
- Decentralization / “no platform lock-in”
- Sharing security requirements & best practices
    - Better threat models & adversarial analysis
        - Multisig changes these significantly!
- Compliance, testing services, security review, certification
    - Outdated certification standards (NIST, etc.)?
    - Liability issues

Ecosystem

- 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 futher discussion
  - Synchronous: Private Signal group
  - Asynchronous: Github discussion area
- Next Silicon Salon?
- F2F at #RebootingWebOfTrust 11 in The Hague?
- Do you like what we are doing here today?
  - Become a ongoing sponsor of Blockchain Commons via GitHub.

Christopher Allen (@ChristopherA)

www.BlockchainCommons.com