FOUNDATION

QUANTUMLINK

A Quantum-Resistant Communication Protocol for Passport Prime and Beyond

Ken Carpenter
CTO, Foundation Devices

QUANTUMLINK OUTLINE

PART 1
WHAT IS THE PROBLEM?

PART 2
PASSPORT PRIME & QUANTUMLINK

PART 3
QUANTUM RESISTANCE

PART 4
QUANTUMLINK UNDER THE HOOD

FOUNDATION

PART 1
WHAT IS THE PROBLEM?

WHAT PROBLEM ARE WE TRYING TO SOLVE?

- Foundation Devices makes a line of air-gapped Bitcoin hardware wallets under the Passport brand.
- Being air-gapped, while a great security practice, comes with some downsides to user experience.
  - Scanning QR codes depends on lighting conditions.
  - Large transactions might contain 100s of QR codes — not practical, so users fall back to microSD.
  - Firmware updates require a microSD card and adapter and many users have trouble formatting the cards properly or downloading & copying the files.

FOUNDATION

OTHER LIMITATIONS OF AIR-GAPPING

- Exchanging data between the wallet and the device for things like Anti-Exfil requires multiple back and forth scans.
- Passport is not able to have up-to-date information on the Bitcoin price, the state of the blockchain or which addresses have already been used.
- Backup of Passport’s metadata (e.g., account labels, multisig config, etc.) is infrequent with air-gapping.

FOUNDATION

PART 2
PASSPORT PRIME &
QUANTUMLINK

FOUNDATION

PASSPORT PRIME - THE IMPETUS FOR QUANTUMLINK

- As we worked on our next-gen device, Passport Prime, we decided that the next billion people to onboard to Bitcoin should not have to live with these limitations.
- We had to find a way to make local wireless communication much more secure.
- After spending a fair bit of time considering the problem and possible solutions, we came up with the idea for QuantumLink.
- We wanted a protocol that would provide all the benefits of an air-gapped security model, but with massive improvements to user experience.

FOUNDATION

HOW DOES IT WORK?

KEY EXCHANGE #1

Prime generates an encryption keypair and an digital signature keypair. The public keys for each of these are shared with Envoy via an animated QR code in Blockchain Commons UR format during onboarding.

More on the types of these keys shortly!

FOUNDATION

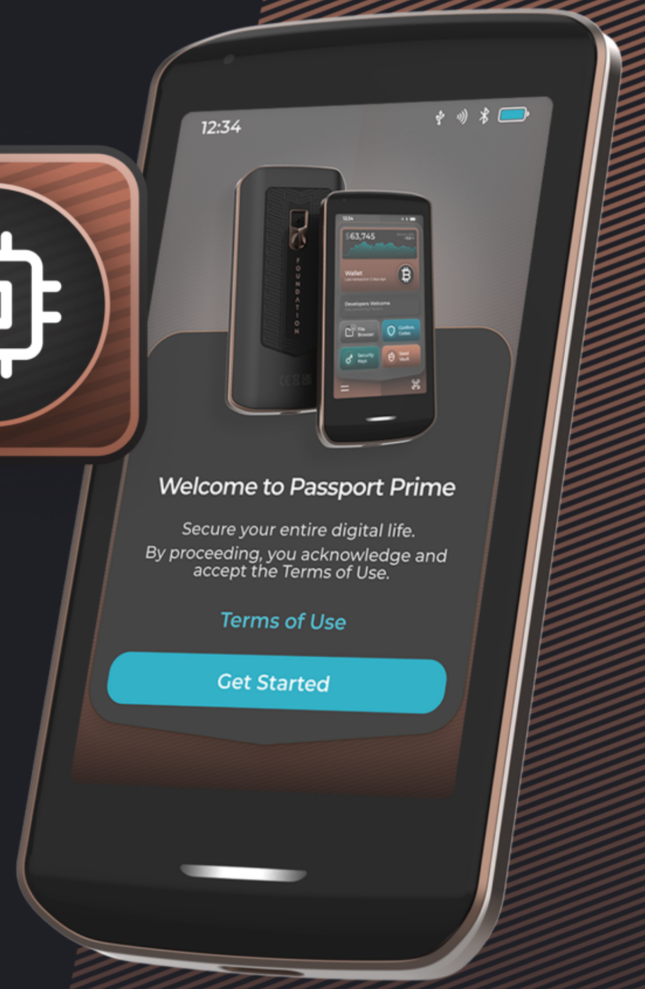
HOW DOES IT WORK?

KEY EXCHANGE #2

Envoy similarly generates its own two keypairs (also for encryption and signatures) and sends the associated public keys to Prime with an encrypted and signed message. Now both sides have the necessary key material and we have established a secure tunnel between Envoy and Prime.

FOUNDATION

PASSPORT PRIME BT CHIP IS A BLACK BOX



ON-DEVICE COMMUNICATION

The main MCU and the BT MCU are separate components. All data is encrypted and signed by the sender before being sent through the Bluetooth chip on Prime, so the BT MCU is unable to modify or inspect any messages in transit.

FOUNDATION

SECURE TUNNEL ACTIVE

Every message has a unique encryption key, which is, itself, encrypted with the receiver's encryption public key. MITM can't inject valid messages or decode received messages.

FOUNDATION

HIGH-LEVEL BENEFITS OF QUANTUMLINK

- Out-of-band key exchange process to create a secure two-way communication tunnel.
- All messages are encrypted and signed.
- Bandwidth is high enough for KeyOS firmware updates or downloads of new apps over the air.
- Passport Prime can be kept up-to-date with external information such as Bitcoin price, blockchain info and used addresses.
- Avoid ECC and similar cryptosystems which are susceptible to Shor’s algorithm.
- In other words, QuantumLink is quantum resistant.

FOUNDATION

PART 3
QUANTUM RESISTANCE
(A BRIEF INTERLUDE)

FOUNDATION

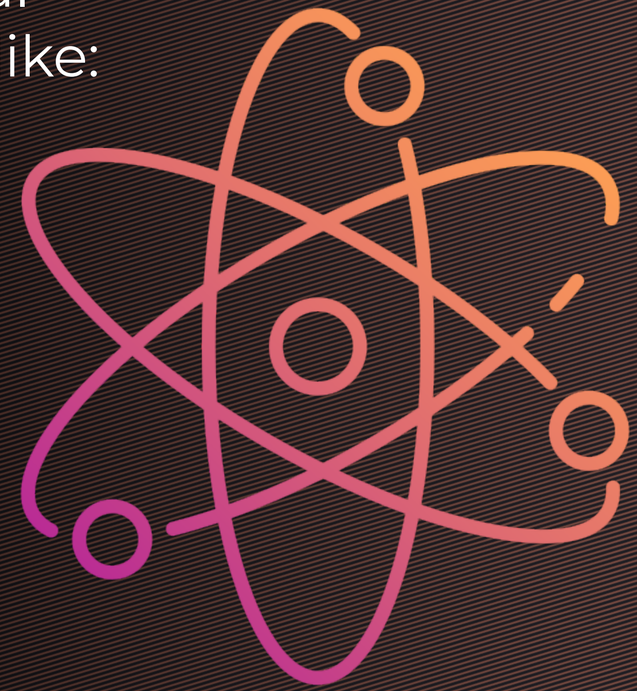
WHAT IS QUANTUM VULNERABILITY?

- First, what is the problem we are solving with QuantumLink?
- Most cryptography and digital signature systems in use today are vulnerable to quantum computers.
- In particular, Shor’s algorithm, when run on a sufficiently powerful quantum computer, can efficiently solve both:
  - Integer factorization (breaks RSA)
  - The discrete logarithm problem (breaks ECDSA, Schnorr signatures, Diffie-Hellman and others)

FOUNDATION

WHAT IS QUANTUM RESISTANCE?

- New systems have been developed based on mathematical problems that remain hard even for quantum computers, like:
  - Lattice-based cryptography
  - Hash-based signatures
  - Code-based cryptography
  - Multivariate cryptography

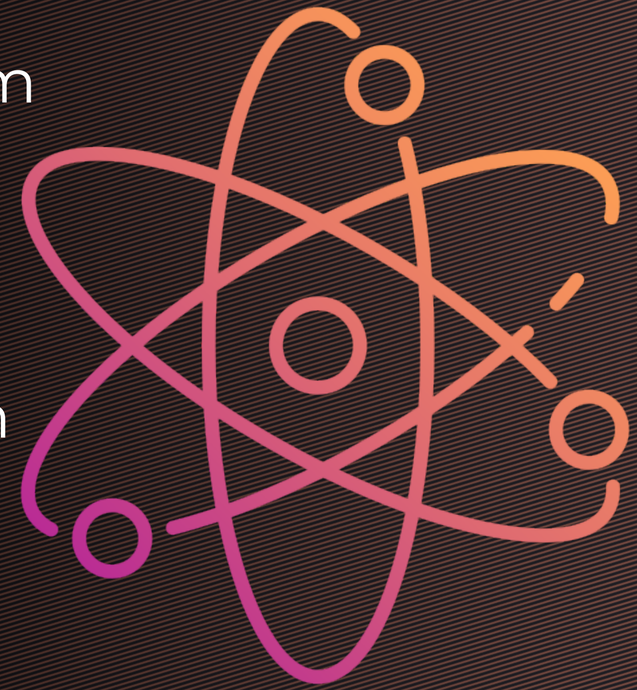


- These new systems are said to be ***“quantum resistant”*** because there are no known algorithms to which these systems are vulnerable.

- This means that even with a powerful quantum computer, the encryption and signature schemes can’t be broken.

WHAT WE CHOSE FOR QUANTUMLINK

- For encryption, we chose **ML-KEM**
  - Module-Lattice-Based Key-Encapsulation Mechanism
  - Formerly called Kyber
  - Not actually used for asymmetric encryption of the payload, but instead is used to encrypt a symmetric encryption key like ChaCha20-Poly1305 or AES-256 in each message



- For digital signatures, we chose **ML-DSA**
  - Module-Lattice-Based Digital Signature Algorithm
  - Formerly called Dilithium

PART 3
QUANTUMLINK UNDER THE HOOD

FOUNDATION

KEY EXCHANGE IN DETAIL - PASSPORT -> ENVOY

- Passport first shows a static QR code with its Bluetooth device address.
- The user scans the QR with their phone’s camera app, and the OS opens Envoy.
- Envoy connects to Prime’s Bluetooth, but doesn’t send any data yet.
- Prime sees this connection, and switches the static QR code to an animated QR code.
- This QR code uses the Blockchain Commons UR standard and contains:
  - XID Document: An eXtensible IDentifier Document (another Blockchain Commons standard) which contains:
    - An eXtensible IDentifier (XID)
    - Prime’s ML-KEM (Kyber) public key
    - Prime’s ML-DSA (Dilithium) public key
  - Additional metadata (e.g., device SKU, firmware version, etc.)

FOUNDATION

KEY EXCHANGE IN DETAIL - ENVOY -> PASSPORT

- Envoy scans the UR from Passport and saves the data.
- Envoy then builds a response message containing:
  - XID Document: An eXtensible IDentifier Document containing:
    - An eXtensible IDentifier (XID)
    - Envoy's ML-KEM (Kyber) public key
    - Envoy’s ML-DSA (Dilithium) public key
  - Current date and time
  - Additional metadata
- Envoy now sends this message over Bluetooth using encryption and a digital signature.
- But what format are these messages that we are sending?

FOUNDATION

MESSAGE STRUCTURE - ENTER GSTP

- QuantumLink is based on the Blockchain Commons Gordian Sealed Transport Protocol (**GSTP**).
- We were aware of GSTP for some time, but it did not yet support post-quantum encryption.
- After some discussion with Blockchain Commons, we decided to engage them to add support for ML-KEM (Kyber) and ML-DSA (Dilithium).
- As usual, they delivered above and beyond, developing a well-architected solution, properly tested, and which “just worked” with very minor code modifications vs. the non-post-quantum version of GSTP we were already running.

Blockchain Commons

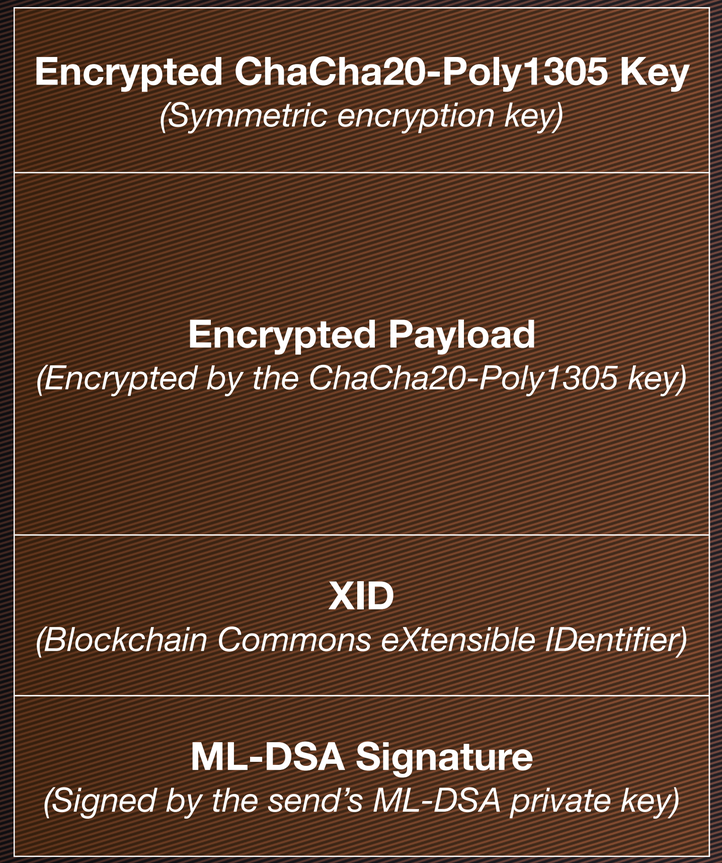
GORDIAN SEALED TRANSPORT PROTOCOL (GSTP)

- We won’t go into too much detail here, but GSTP is a request/response protocol built on top of the Blockchain Commons *Gordian Envelope* standard.
- Envelopes provide a clean and composable way of building protocols that can easily include encrypted data or signatures, or elide data while maintaining the same hash tree, and a lot more.
- Envelopes + GSTP form a great foundation on which to build QuantumLink.

Blockchain Commons

HOW IS EACH MESSAGE STRUCTURED/PROCESSED?

- Each GSTP message is structured as shown.
- Upon receiving a message, the validation process is as follows:
  - Decrypt the ChaCha20-Poly1305 key using the ML-KEM private key on the receiver.
  - Decrypt the payload using this ChaCha20-Poly1305 key.
  - Check the signature of the decrypted payload vs. the provided ML-DSA signature.
  - We lookup the right public keys to use to perform the decryption and to validate the signature using the XID included in the message.
- If any of these steps have an error, the message is dropped.



FOUNDATION

CURRENT QUANTUMLINK MESSAGES

- We built our own custom messages on top of GSTP to exchange between Envoy and Prime.
- Initially, these include:
  - Synchronizing the onboarding flow - Envoy tells Passport what step of onboarding to move to and vice versa
  - Signing Bitcoin transactions
  - Updating the current date, time and time zone
  - Updating the current Bitcoin price
  - Installing firmware updates
  - Installing new Passport Prime apps *(App SDK coming later in 2025)*

FOUNDATION

FUTURE QUANTUMLINK MESSAGES

- In the future, we will also likely add support for:
  - Other currency prices
  - Relevant UTXOs
  - Used addresses
  - Blockchain metadata
  - Multisig setup data

- Let us know if you have a specific use case in mind or grab the SDK later this year and implement whatever you want to see!

KEY STORAGE, LIFETIME & SECURITY

- On Passport Prime, we store the private & public keys (ML-KEM and ML-DSA) for each Envoy connection in an encrypted file. We use AES-256 encryption, and the associated encryption key is derived from entropy stored in Prime's ATECC608C secure element.
- On Envoy, we store the keys in the iOS Key Manager or the Android Keystore.
- We currently perform a single public key exchange at the time of initial pairing (the QR code process shown previously). There is no formal key rotation procedure, but a user can delete the associated keypair from Prime and reconnect with a new keypair at any time.
- We may implement automatic key rotation in the future.

FOUNDATION

ADDITIONAL POINTS ON SECURITY

- The Bluetooth chip (Nordic nRF 52805) is running a vendor-supplied “soft device” Bluetooth stack (binary blob) with a custom app.
- The custom app connects to Prime’s main processor (Microchip SAMA5D28) over a SPI connection.
- Any messages received by Prime must be properly signed and encrypted by a known partner (initially just Envoy) identified by the XID.
- The Bluetooth chip is treated as a black box. It is not capable of MITM attacks that would alter or replace messages (well, it could grief, but any such messages would be discarded).

FINAL POINTS

- All the Blockchain Commons protocols mentioned are Open Source!
  - GSTP, UR, Envelope, XID
- All Passport Prime apps, the Envoy mobile app, and the KeyOS operating system, including the QuantumLink protocol, are Open Source (GPL3 or compatible).
- Foundation will document the QuantumLink protocol message formats, as well as a mechanism for adding custom messages later in 2025.
- The Prime SDK is also coming later in 2025, but if you want to get a head start, get in touch and we may be able to work with you sooner.

open source initiative

FOUNDATION

Q & A

Learn more about Passport Prime at:

https://foundation.xyz/passport-prime

FOUNDATION