The EVM relies on digital signatures for transactions to be authenticated, which are currently implemented via an elliptic curve (EC) cryptography scheme, ECDSA. Quantum computing, via Shor's factorization algorithm, breaks ubiquitous encryption protocols such as RSA and EC. As a consequence, national security agencies such as NSA, ANSSI, BSI have been seeking new algorithms which cannot be broken by a quantum computer, termed post-quantum (PQ) algorithms (see e.g. NIST competition), as well as releasing guidelines on the migration to quantum resistant encryption standards. Indeed, active research and development in quantum computing lead many to believe that the materialisation of such a threat is within the next decade.

We propose a new transaction type 'Q' (decimal 81, hexadecimal 0x51) for the EVM, whereby transactions are signed using both an ECDSA and a PQ signature (deterministic CRYSTALS- Dilithium Level 2). This hybrid approach is in line with suggested mandatory practices put forth by government agencies, enables a smooth transition, is backward compatible and ensures stronger security than PQ signatures alone, as these have not been scrutinised as much as their classical counterparts.

More precisely, the sender of a transaction would submit current signature parameters (ECDSA signature) as well as:

- PQ signature,
- PQ public key (as it can not be recovered from the signature itself),
- Hash of both signatures.

The additional transaction information is held until the finality is reached (e.g., 6-10 blocks). After that, only the hash of the two signatures is stored in addition to the data that is stored for transactions of type 1. This saves space (as the PQ signature and public key are significantly larger than the ECDSA signature) and offers the same level of security as the transactions cannot be modified due to the chaining of the block hashes.

Introducing the new transaction type will have an impact on the space requirements for storing the additional transaction information and block processing time for miners and validators when validating new transactions. Indeed, the proposed PQ signature and public key are respectively 21 and 38 times larger than the ECDSA signature, i.e. roughly 60 times greater in total. Since the PQ signature and the corresponding public key do not get stored to the block chain and only the additional hash value of the two signatures is stored, the increase in size of the stored data is about 8% for a typical transaction (see section 3.4 of the paper for a full argument). Thus, given cryptographically relevant quantum computers, adding PQ signatures significantly improves the security of the EVM-based block chains, and so it can be argued that this increase in transaction size is acceptable given today's hardware capacities.

This hybrid PQ scheme proposes an efficient and simple solution to the quantum threat for the EVM via the addition of a PQ signature. Recall that n

-bit classical (quantum) security means that it would take a classical (quantum) computer 2^n

operations to break. Currently, 80-bit security is considered safe. ECDSA using the SECP-256k1 curve has 128-bit classical security and about 30-bit quantum security, i.e. it is not quantum resistant. In contrast, dCDL2 has 123-bit classical security and 112-bit quantum security, has just been standardized by NIST and is thus considered safe in the presence of both classical and quantum computers.

Full details of the proposal here.