QRL Documentation

Release latest

May 26, 2017

Contents

#The Quantum Resistant Ledger - TheQRL

Python-based blockchain ledger utilising hash-based one-time merkle tree signature scheme (XMSS) instead of ECDSA. Proof-of-stake block selection via HMAC_DRBG PRF and a signed iterative hash chain reveal scheme.

Hash-based signatures means larger transactions (6kb per tx, binary), longer keypair generation times and the need to record 'state' of transactions as each keypair can only be used once safely. Merkle tree usage enables a single address to be used for signing numerous transactions (up to 2^13 computationally easily enough). Transactions have an incremented nonce to allow wallets to know which MSS keypair to use - currently Lamport-Diffie and Winternitz one-time signatures as part of merkle signature schemes and XMSS/W-OTS+ are natively supported.