

CRYPTO ALLIANCE



CRYPTOALLIANCE



SPHINX

<https://linktr.ee/sphinx.org>

An open-source post-
quantum blockchain layer 1

Problem of Large scale QC threat into primitive cryptography;

1. EC(DH, DSA)/ RSA will be broken =
 - Shor's algorithm in $O((\log N)^3)$
2. Hash-Function SHA2/3 $y^{2^{256}} = H0(h^{2^{256}}(x))$ will be broken =
 - Grover's algorithm in $O(2^{256/2})$
 - BHT algorithm in $O(2^{256/3}) + \text{qRAM}$
3. AES will be broken =
 - Grover's algorithm in $O(2^{256/2})$
 - BHT algorithm in $O(2^{256/3}) + \text{qRAM}$
4. Deterministic CSPRNG will be broken =
 - Grover's search in $O(\sqrt{N})$
5. Passphrase 2048^{12} might be broken =
 - Grover's algorithm in $O(2048^{12/2})$
 - BHT algorithm in $O(2048^{12/3}) + \text{qRAM}$

Solution of Large scale QC is only migration into PQC;

1. HBS will give us $O(2^{128}) \approx 2^{52}$ years against QC
2. Hash-Function $y^{2^{256*2}} = H_0(h^{2^{256}}, h^{3^{256}}(x))$ increase hardness against =
 - Grover's algorithm in $O(2^{\frac{256}{2}*2})$
 - BHT algorithm in $O(2^{\frac{256}{3}*2}) + \text{qRAM}$
3. AES + FHE might help against =
 - Grover's algorithm in $O(2^{256/2})$
 - BHT algorithm in $O(2^{256/3}) + \text{qRAM}$
4. qRNG will help but there is no individual hardware exist yet =
 - Grover's search in $O(\sqrt{N})$
5. Passphrase 2048^{12} + Base32Passkey $2^{4199040*8}$ will help =
 - Grover's algorithm in $O(2048^{12/2}) + O(2^{4199040*8/2})$
 - BHT algorithm in $O(2048^{12/3}) + O(2^{4199040*8/3}) + \text{qRAM}$

Roadmap;

1. Build team (Founder, Co-founders, Engineers).
2. Qrypto Alliance Legal registration || Sphinx Foundation.
3. Website Development.
4. Global Community Developmet.
5. Adjust/ Accelerate existing idea and code base.
6. Technical Development ⇒ Relase Whitepaper.
7. Raising Fund.
8. PoS (SNOW), SVM, MPC/ MPS, ZK, PQC ⇒ Blockchain development.
9. 100M **\$SPX** Coins Issuance.
10. Testnet.
11. Mainnet.