Challenges of the Transition of Blockchain to Quantum-Safe

Author(s) : Ludovic Perret

The purpose of this document is to the sketches some ideas for a white paper around blockchains and quantum-safe cryptography. In 2021, the group already published a document [Blockchains in the Quantum Era](https://cloudsecurityalliance.org/artifacts/blockchains-in-the-quantum-era/). We give below the table of contentsBlockchain Overview

* 1. What is a Blockchain?
  2. How it All Started: Bitcoin and Cryptocurrencies
  3. A New Paradigm: Smart Contracts
  4. Emerging Blockchain Applications

1. The Quantum Era
2. Main Cryptographic Tools for the Blockchain
   1. Random Number Generation
   2. Hash Functions .
   3. Public-key Signatures
3. Risk Analysis on a Few Blockchains
   1. Bitcoin
   2. Ethereum
   3. Hyperledger Fabric (HLF)
   4. Zcash
4. Future Solutions
   1. Quantum-Safe Signatures and Encryption
   2. Attributes of Post-Quantum Blockchain Signatures
   3. Post-Quantum Signatures under Standardization
   4. Quantum Blockchains
5. Conclusion: Transition from Pre-Quantum to Post-Quantum Blockchain

The proposal is to write a new with paper “Challenges for Transitioning of Blockchains to Quantum-Safe Cryptography. It should be then as a follow-up of the previous white paper. The topics that could be covered include :

* More detailed statements about the impact of Shor’s on ECDSA and Grover’s to the Proof-of-Work
* Discuss the pros and cons of distinct transition approaches
  + Ignore the threat and do nothing
  + Propose ad-hoc techniques for preventing the risk such as the P2PKH for Bitcoin, stealth adress, etc
  + Updating the non-quantum safe components
    - New pq signature and its impact (public and private blockchains)