Impact of post-quantum signatures on blockchain and DLT systems

Stephen Holmes

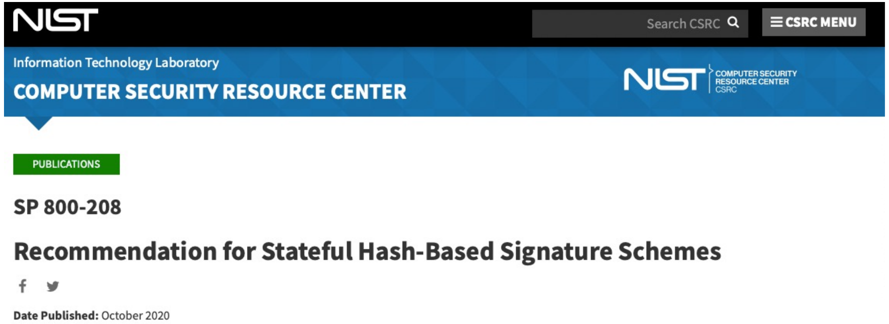
DLT2023 - 26 May 2023

Motivation

US National Institute of Standards and Technology (NIST) published post-quantum digital signature algorithms for standardization

<u>**Stateless post=quantum signatures**</u>

<u>**Stateful post=quantum signatures**</u>



What would be the impact of changing signature scheme in blockchain or DLT systems from ECDSA to any of these post-quantum signatures?

…. (this paper)

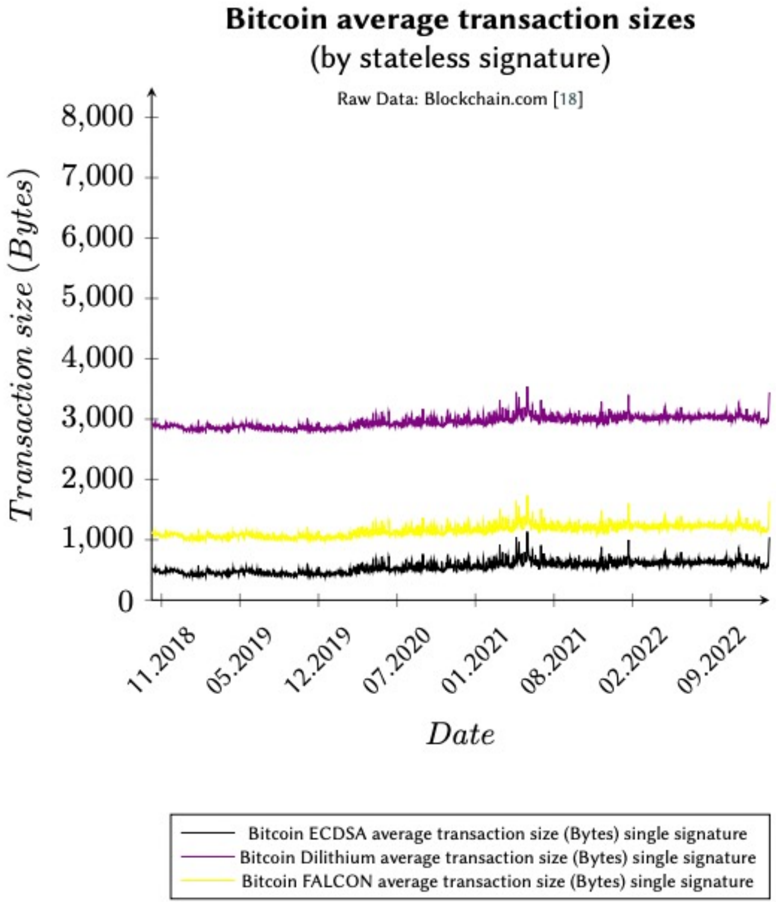
Approved NIST post-quantum digital signatures

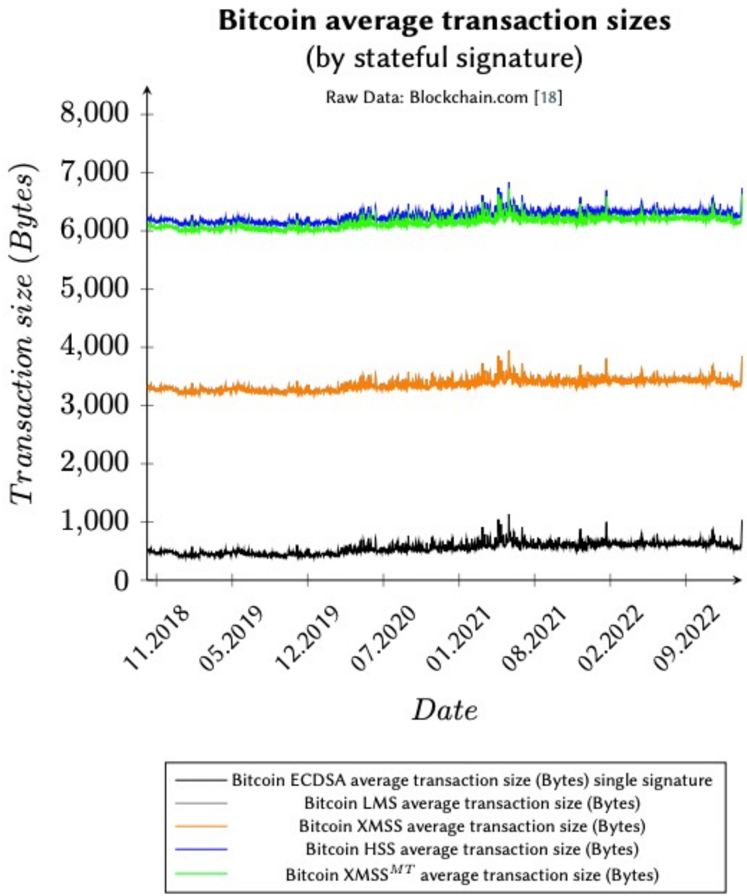
Signature scheme	Post-quantum security level (bits)	Type	Underpinning technology	Secret signing key (bytes)	Public key (bytes)	Signatures size (bytes)
ECDSA – today	128 Pre-quantum	Stateless	Elliptic curve	32	32	32
Dilithium	128	Stateless	Lattice	1312	2528	2420
FALCON	128	Stateless	Lattice	897	1281	690
Sphincs+	128	Stateless	Hash	32	64	17,088
LMS	128	Stateful	Hash	32	56	2828
XMSS	128	Stateful	Hash	32	68	2820
$XMSS^{MT}$	128	Stateful	Hash	32	68	5605
HSS	128	Stateful	Hash	32	60	5716

Methodology and approach

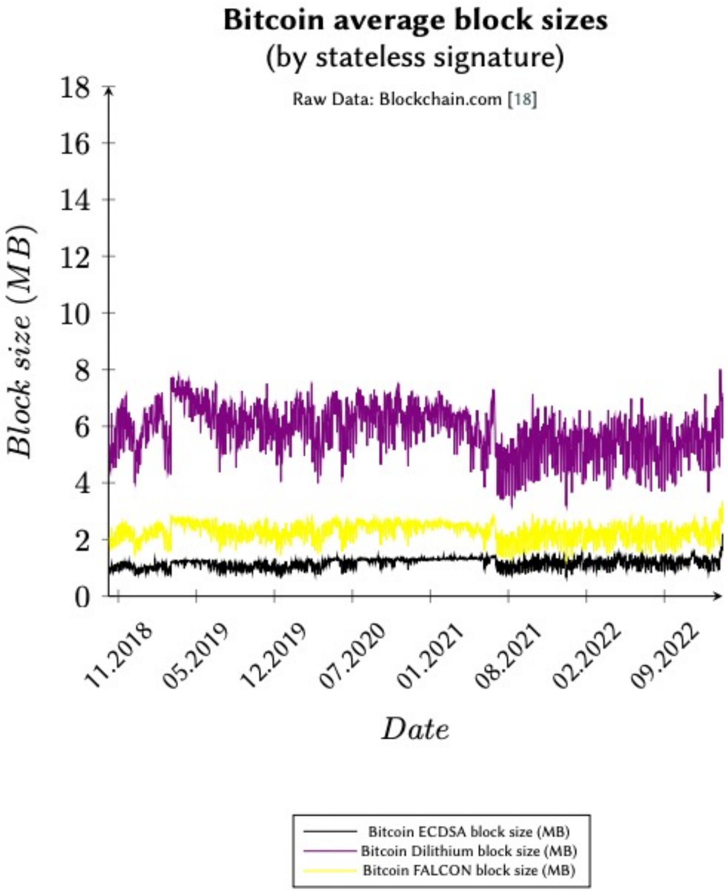
- Using data from historical bitcoin transactions
  - Re-tread transactions to remove ECDSA signatures and replace with post-quantum signatures.
  - Assume in post-quantum blockchain we use SHA384 not SHA256 for public key hash stored on blockchain
  - Use post-quantum signatures with same relative security as ECDSA signatures
- Blockchain and DLT systems are optimised ecosystems
  - Assume the blocksize is optimised for each bitcoin/DLT system
- Evaluate the impact of adopting post-quantum signatures:
  - Transaction sizes
  - Block sizes
  - Number of transaction in existing block size

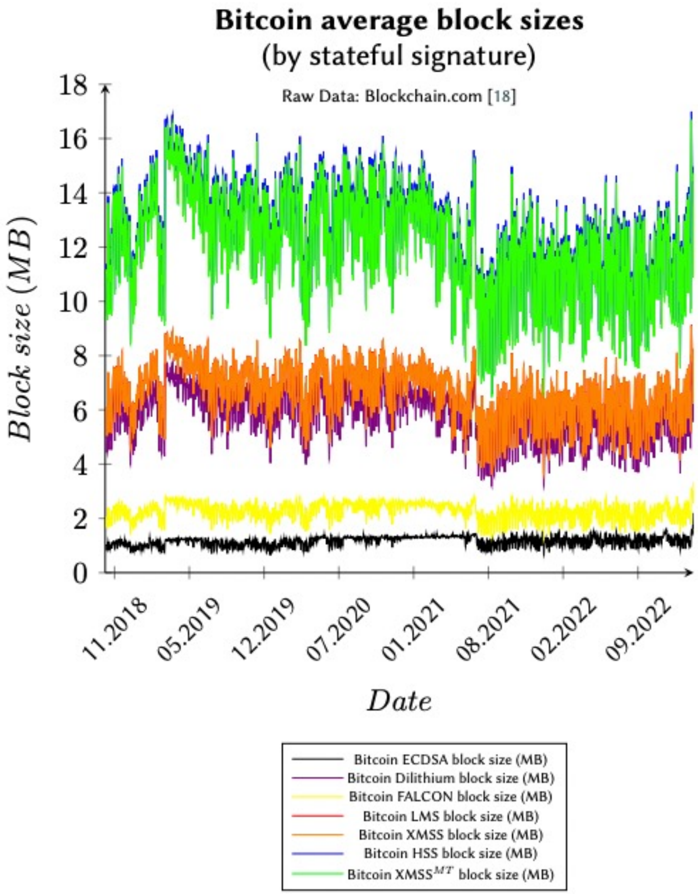
Signature impact on transaction sizes



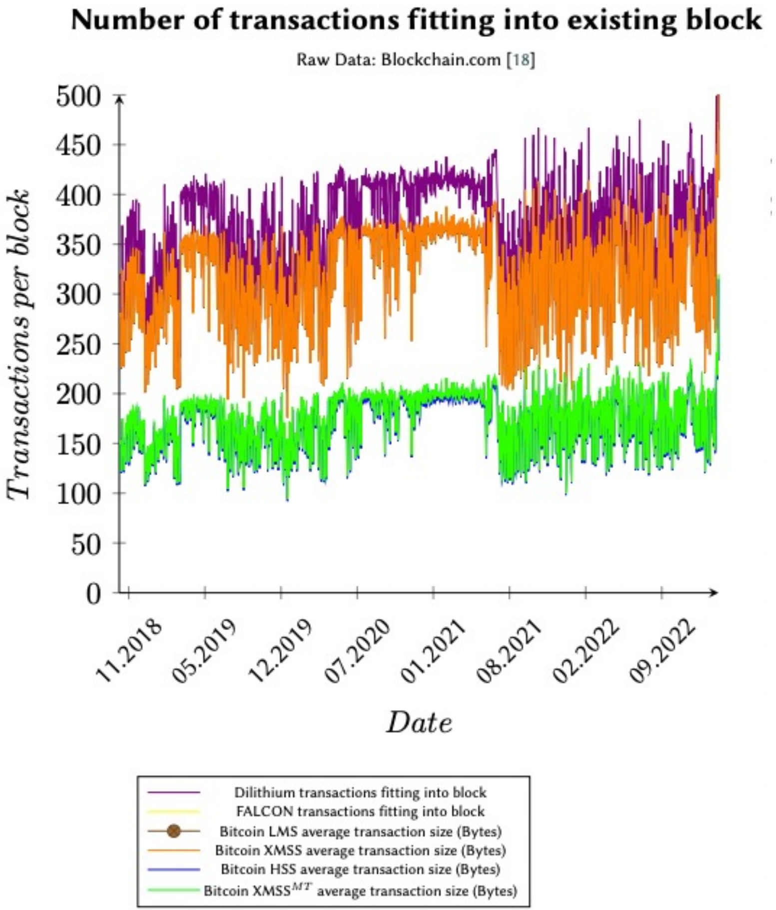


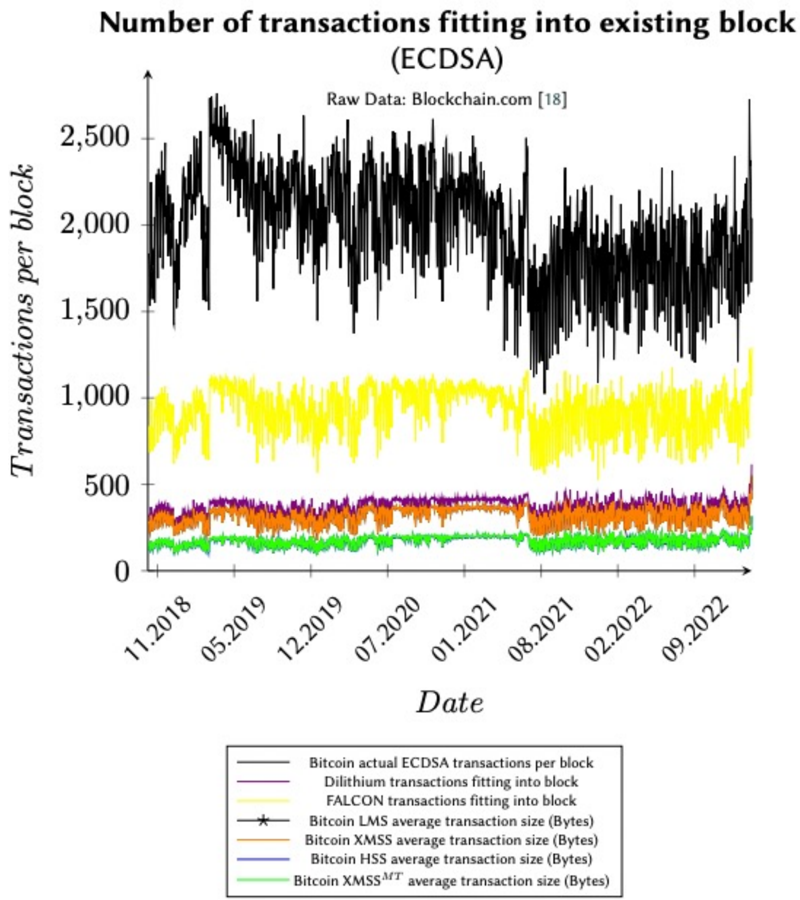
Signature impact on block size





Number of transactions per 1MB block





Impact of post-quantum signatures on blockchain & DLT systems

	Bitcoin	Dilithium	FALCON	Sphincs256	LMS	XMSS	HSS	$XMSS^{MT}$
Average txn size (Bytes)	552 1x	2956 5x	1154 2x	17624 32x	3364 6x	3356 6x	6252 11x	6140 11x
Average re-calculated block size (MB)	1.165 1x	5.88 5x	2.284 2x	35.108 30x	6.688 6x	6.672 6x	12.45 11x	12.223 11x
Number of transactions fitting into existing block	1993 1x	365 0.18x	939 0.47x	60 0.03x	321 0.16x	322 0.16x	172 0.08x	175 0.08x

Summary

- The NIST recommended post-quantum signatures are not drop-in replacements for blockchain and DLT systems
  - Signature sizes are significantly larger
  - Most schemes have larger key sizes and/or larger signatures
- Stateless post-quantum signatures lack some of today’s ECDSA functionality
  - No threshold-signature capability
  - No equivalent to ECDSA recover (public key can be recovered from signature)
- Number of blockchain/DLT transactions will be reduced
  - Layer-2 transaction roll-up protocols may become a critical component
  - But… need to be post-quantum too!

Looking forward…

- NIST are continuing the post-quantum signature competition

NIST announced that the PQC standardization process is continuing with a fourth round, with the following KEMs still under consideration: BIKE, Classic McEliece, HQC, and SIKE. However, there are no remaining digital signature candidates under consideration. As such, **NIST is calling for additional digital signature proposals to be considered in the PQC standardization process. Submission packages must be received by NIST by June 1, 2023.**

- Security evaluation and attacks are on-going for post-quantum signatures
    - Upgrading a blockchain to a new signature scheme is disruptive
    - We may choose a higher level of security to give margin for these attacks
        - ❖ Lattice based cryptography has a long history of attacks that weaken effective security
        - ❖ But… this will further negatively impact a blockchain or DLT system

Thank you!
Questions?

Stephen.holmes@surrey.ac.uk

Recap - Quantum Computer threat model

- Digital Signatures underpin security of blockchain and DLT systems
    - Blockchain and DLT systems use Elliptic Curve Digital Signature Algorithm
    - Elliptic curve signatures based on mathematical hard discrete logarithm problem
        - Hard problem for today's computers
        - Easy problem for quantum computers running Shor's algorithm

- Transaction submitted to blockchain/DLT system include public key and signed message (proving sender has access to private key)
    - Quantum adversary can derive private key from public key in a transaction
    - By cracking private key can submit transaction to steal assets by signing new transaction with private key and divert to adversaries account

- Blockchain's depend upon cryptographic hash algorithms to be secure
    - NIST advice is to move from SHA256 to SHA384