

Impact of post-quantum signatures on blockchain and DLT systems

Stephen A. Holmes^{1,*,\dagger}

¹University of Surrey, FEPS, Stag Hill, University Campus, Guildford GU2 7XH, UK

Abstract

Blockchain and Distributed Ledger Technologies (DLT) are accelerating in deployment and increasingly being used to securely store digital assets. As the world digitises, there will be an acceleration of asset tokenisation with new marketplaces created for fractionalised tokenised digital assets. Blockchain and DLT systems using ECDSA signatures are vulnerable to a quantum adversary. The NIST post-quantum cryptography competition and the NIST stateful hash-based signature recommendations were used to determine the impact of using any of the proposed NIST finalist quantum-safe digital signature schemes. We examined the impact on both block sizes and block interval times that would be required if today's ECDSA signatures were replaced by a NIST post-quantum signature scheme. We observed that the increased cost of adopting a cryptographic scheme has a significant negative impact on blockchain storage and communications costs. This research illustrates the need for smaller, more efficient cryptographic signature schemes that are closer to the size of the currently deployed ECDSA signatures and supports the adoption of layer-2 blockchain and layer-2 rollup protocols to mitigate the cost and increase the transaction throughput of the post-quantum blockchain or DLT system.

Keywords

Blockchain & Distributed Ledger Technology (DLT), quantum-safe blockchain, post-quantum digital signatures, ECDSA signatures, Stateful post-quantum hash based signatures

1. Motivation and contribution

Blockchain and Distributed Ledger Technologies (DLT) are accelerating in deployment and are increasingly being used to securely store digital assets. As the world digitises, it is increasingly tokenising these assets, and new marketplaces are being created for fractionalised tokenised digital assets. Assets under blockchain management are accelerating and the value of these tokenised assets is growing rapidly.


The technology of blockchains and DLT systems has evolved over time. However, the core security of any blockchain and DLT system is the strength of the digital signature that is used to ensure that only the person with the secret key to generate a signature that matches a public key for a transaction message can unlock and execute the transaction.


Today's blockchain and DLT signature schemes are vulnerable to a quantum adversary [1, 2]. Shor's algorithm [3] can recover the secret key from a public key used in the message signature, undermining the security of any existing blockchain or DLT system using today's ECDSA

DLT2023, May 25–26, 2023, Bologna, Italy

 s.a.holmes@surrey.ac.uk (S. A. Holmes)

 0000-0003-4024-8265 (S. A. Holmes)

 © 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

signature schemes. The underlying risk is the need to disclose the public key at the time of submitting a transaction to the blockchain. The public key is secure on the blockchain itself because only the hash of the public key is transmitted and stored on the blockchain, which makes this aspect quantum-safe. The danger occurs when a transaction is submitted to the blockchain. A quantum adversary, using Shor's algorithm, can derive the secret key from the public key in the transaction and sign a front-running transaction to steal an asset. Once the transaction is finalised on the blockchain, when finality is reached, the transaction is protected from a quantum adversary.

Our contribution is an analysis of the impact on both block sizes and number of transactions per block that would be required if today's ECDSA signatures were replaced by a post-quantum signature scheme. Our overall finding after replaying existing transactions with post-quantum signatures is that the number of transactions per block is a factor of 2 to 32 times smaller with the same block size. We note that blockchains and DLT systems are fine-tuned systems and the transaction message sizes, block sizes, and block interval times have been incrementally optimised over time. Our research highlights the significant additional cost of adopting a post-quantum signatures scheme and illustrates the need for smaller, more efficient post-quantum signature schemes for blockchain and DLT systems. We note that, for some blockchains, it is possible to simply decrease the block interval time. However, for other blockchains, this is not practical. For example, bitcoin's block interval time is 10 minutes, so you could simply change this to one minute. However, most modern blockchains and DLT systems have block interval times of around 15 seconds, so changing the block interval time will not be a practical solution for most blockchains. This supports increased adoption of layer-2 protocols, such as roll-ups, that batch transactions off-chain and commit roll-ups on-chain to layer-1 native blockchains, scaling transaction throughput, and reducing costs. However, both layer-1 native blockchains and layer-2 roll-up protocols need to be post-quantum secure.

2. Analysis of post-quantum signature impacts on blockchain

We examined the post-quantum cryptography finalist signature schemes from the NIST post-quantum cryptography competition and the NIST stateful hash-based signature recommendations to determine the impact of upgrading from today's non-quantum-safe signature schemes. The proposed post-quantum signatures lack a couple of features that the blockchain takes for granted today. Namely, there is no equivalent functionality for ECRECOVER that is used today in blockchain to recover the public key from a signature without the need to send the public key in order to reduce message sizes. All proposed NIST post-quantum finalists lack the ability to create threshold based signatures [4] which is commonly used in blockchain to enable delegation of signing authority to multiple parties where a threshold number of signatures is required to execute a transaction, for example, 3 out of 5 signatures required.

2.1. Post-quantum signatures

The finalist candidate signature schemes from the US National Institute of Standards and Technology (NIST) [5, 6, 7] Post Quantum Cryptography competition all have one thing in

common. That is, signatures larger than the current elliptic-curve ECDSA signature schemes used by the current blockchain and DLT systems.

The NIST security levels for each post-quantum algorithm are specified in table These, in turn, impact the size of the parameters input to each algorithm to meet the security requirements, which, in turn, impacts key sizes and signature sizes.

NIST have standardised 3 stateless signatures schemes and 2 stateful hash based signature schemes in 2020. The NIST standards for stateless signatures specify 3 algorithms: Dilithium, Falcon and Sphincs. The NIST standards for stateful signatures specifies two algorithms that can be used to generate a digital signature, both of which are stateful hash-based signature schemes: the Leighton-Micali Signature (LMS) system and the eXtended Merkle Signature Scheme (XMSS), along with their multi-tree variants, the Hierarchical Signature System (HSS) and multi-tree XMSS (XMSS^{MT}).

Table 1
NIST PQC signature finalists level 1 security and NIST stateful hash-based signatures

Signature scheme	Underpinning technology	State	Private Key (bytes)	Public Key (bytes)	Signature (bytes)
ECDSA (today's blockchain)	Elliptic curves	Stateless	32	32	32
Crystals - Dilithium2 [8]	Lattice-based (MLWE/MSIS)	Stateless	1,312	2,528	2,420
FALCON512 [9]	Lattice-based (NTRU)	Stateless	897	1,281	690
Sphincs+ SHA256-256f Simple [10]	Hash Based	Stateless	32	64	17,088
Leighton-Micali Signature (LMS)[6] $w = 16, p = 67, 2^{20}$ max signatures	Hash Based	Stateful	32 (n)	56 (24 + n)	2,828 (12 + n(p + h + 1))
eXtended Merkle Signature Scheme (XMSS)[6] $w = 16, p = 67, 2^{20}$ max signatures	Hash Based	Stateful	32 (n)	68 (4+2n)	2,820 (4+np+h+1)
Hierarchical Signature System (HSS)[6] 2^{40} max signatures (2 levels)	Hash Based	Stateful	32 (n)	60 (2n-n)	5,716 ((36d + 2nd - n - 20) + n(Σ p + Σ h))
multi-tree XMSS (XMSS ^{MT})[6] 2^{40} max signatures (2 levels)	Hash Based	Stateful	32 (n)	68 (4+2n)	5,605 (Σ h/8) + n(Σ p + Σ h + 1)

Impact of migrating to NIST PQC candidate signature schemes

We examined the finalist NIST PQC candidate signatures [5] and NIST recommended stateful Hash-based signatures [6] and used the key sizes and signature sizes at level 1 security to apply to existing bitcoin transactions to determine the impact of replacing today's ECDSA signatures with a NIST signature candidate.

Impact of block size on blockchain performance

The impact of the block size and associated transaction size has been a constant debacle for most blockchain developers. A larger block size will require a longer transmission time, as compared to a smaller block size. A smaller block size will require a longer block composition time to clear all transactions compared to a larger block size. Both performance factors are contradictory to each other, implying that if one value increases, then the other value decreases, and vice versa. In order to improve the performance of the network, a suitable/or optimal number of transactions should be kept in each block (block size) so that transmission time and block composition time are minimised. Singh et al. [11] identify a set of mathematical descriptions of the task and that these are not single objectives but conflicting multiple objectives and use multiple objective optimisation (MOO) techniques to solve these for a specific blockchain and determine the optimal block size.

Impact of signature private key size

The size of the private key for digital signatures on the blockchain affects a blockchain or DLT system in two important ways. The digital private signing key needs to be stored securely off-chain, and this has traditionally been achieved by using a secure wallet. The private key should never leave the wallet and should only be used to sign a blockchain or DLT transaction. Hardware wallets are typically off-line storage devices with a Hardware Security Module (HSM) and do not have large memories or large processing capacity. Consequently, this would require much larger memory for wallets and limit the number of transactions a wallet could hold. Stateful hash-based signatures can reconstruct the private key from a seed and rely on the strength of the Pseudo-Random number generator available to the wallet.

Impact of signature public key size

The size of the public key for the digital signatures of the blockchain affects a blockchain or DLT system in two important ways. Every blockchain or DLT transaction contains the public key and needs to be transmitted as an unprocessed transaction to all blockchain mining nodes and stored on the blockchain within a block. The identity of a wallet is the public key, and this is stored as a hash of the public key on a blockchain and DLT system; consequently, the size of the public key does not directly impact the blockchain identity. In our model we have changed the hash function from a 256bit output to a 384bit output in line with NIST recommendations for post-quantum hash algorithms. Unprocessed transactions will grow in size and impact the bandwidth and speed of unprocessed transactions delivery. The transaction itself will be recorded on the blockchain and consequently affect the amount of storage required in the block it is placed in. The size of the public key is only relevant when a transaction is sent to the blockchain. Otherwise, the hash of the public key is stored on the blockchain, therefore, not impacting storage on the blockchain.

Impact of signature size

The size of the signature impacts both the size of the unprocessed transaction and the storage size of the transaction placed on the blockchain in a block. The signature is used to sign a transaction to prove that the author of the transaction has access to the signing private key associated with the public key, enabling the assets contained in the public key (blockchain address) to be opened and the transaction accepted for processing. Signatures, along with public keys, are stored on the blockchain as part of the transaction record.

Table 2
Comparison of blockchain maximum block sizes

Blockchain/DLT	Comment	Max block size (MB)
Bitcoin [12]	Started at 1MB increased over time	4
Bitcoin Cash [12]		Designed for 32MB 32
Ethereum [13]	Limit of block size set by Max gas consumption for a transaction and gas price total gas limit for all transactions in a block is 30 million gas	0.91844 (Maximum block size) August 21 2021
CORDA [14]	maxTransactionSize specifies the maximum size for a LedgerTransaction (i.e. fully-resolved transaction including attachments).	4
Hyperledger [15]	No hard limit but performance degrades with block size	No limit

Combined impact of public key and signature size

The biggest impact of the combined size of the public key size and the signature size is the space required for a transaction in a block. The space in a block is precious and the size of the block impacts the overall performance of the system. Block sizes are carefully crafted to maximise the performance of a blockchain or DLT system.

Proof of Stake

This research focusses on the impact of changing the signatures scheme on a blockchain. One area we note but have not explored to date is the impact of moving to a Proof of Stake consensus mechanism, where staking requires quantum safe signatures. This will add an additional post-quantum signature requirement.

Grover's impact on hash security

The impact of Grover's algorithm effectively halves the security of the hash output length. NIST have recommended move to SHA384 to ensure post-quantum security. We took this into account for the transactions and pay to public key hash storage in a block. However, the move to SHA384 requires a major upgrade to the blockchain addressing scheme and if a Proof of Work (POW) consensus is used, a migration from today's SHA256 to SHA384.

2.2. Retreading bitcoin transactions with NIST PQC signatures

To determine the impact of use of NIST post-quantum signature finalist algorithms, we examined three years of bitcoin transactions and block sizes. This information is readily available from a bitcoin block explorer web application and in this case Bitcoin.org data from downloading a full node and calculating these raw data for the following:

- The average block size over the past 24 hours in megabytes.
- Average number of transactions per block over the past 24 hours.

From these two data points, we can calculate the average transaction size per block. Given that there are a number of different transaction types, we can examine the impact of updating the signature scheme from today's ECDSA to a NIST PQC finalist signature scheme. In order to unlock and "spend" a bitcoin, you need to provide the public key of the user owning the bitcoin and sign the transaction with the private key tied to the public key. Addresses sent are public-key hashes to protect the public-key address on the blockchain. We note that this is the best-case scenario with the underlying assumption that all transactions are single signatures. Many transactions will be multisignature transactions and if we were to implement these today, we would use the taproot approach of Schnorr signatures [16, 17] to eliminate the need to store multiple signatures in a block.

$$i = \text{block number}_{\text{start of day}} \quad (1)$$

$$j = \text{block number}_{\text{end of day}} \quad (2)$$

$$\text{daily block size} = \sum_{i..j} \text{size}(\text{block}_x) \quad (3)$$

$$\text{daily blocks} = j - i \quad (4)$$

$$\text{block header size} = 80 \quad (5)$$

$$\text{daily average block size} = \left(\frac{\text{daily block size}}{\text{daily blocks}} \right) - \text{block header size} \quad (6)$$

$$\text{daily average transaction size} = \left(\frac{\text{daily average block size}}{\text{average transactions per block}} \right) \quad (7)$$

We recalculated the average daily block size by calculating the average size of a transaction by dividing the average blocksize minus the block header size (80 bytes) by the average number of transactions per block. Then given the average transaction size, we can recalculate the transaction size based upon the revised size of both the post-quantum signature public key and the signature size. We note that only FALCON has a block size less than 4MB. In 2017, Bitcoin’s block size limit was replaced by a block weight limit of 4 million “weight units.” This changed how data in blocks is “counted”: some data weighs more than other data. Represented an effective block size limit increase: Bitcoin blocks now have a theoretical maximum size of 4 megabytes and a more realistic maximum size of 2 megabytes. This limitation means that even FALCON has larger than 2MB block sizes for the same number of transactions.

We subtract the number of bytes for the ECDSA public key (32 bytes) and also subtract the number of bytes from the ECDSA signature (32 bytes) and replace them with the addition of the SHA384 hash of the PQC public key (bytes) and the PQC signature (bytes). This then gives a view of the revised average transaction sizes (see Figure 1). Note Sphincs+ SHA256-256f simple was excluded from the graph because it produced an infeasibly large transaction size for the blockchain. We note that all NIST currently proposed replacement post-quantum signatures do not support threshold signatures. If we were to include multi-signature transactions (i.e. require multiple signatures for a transaction), then this would further reduce the number of transactions possible in a given target block size. From the average transaction size (adjusted for the PQC signature finalist), we can recalculate the average block size per 24 hours (Figure 2).

Table 3

Summary comparison of post-quantum signatures

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

To maintain the same level of performance based on the same block size as bitcoin, we can restrict the size of the block to the block size shown on average over each 24 hour period;

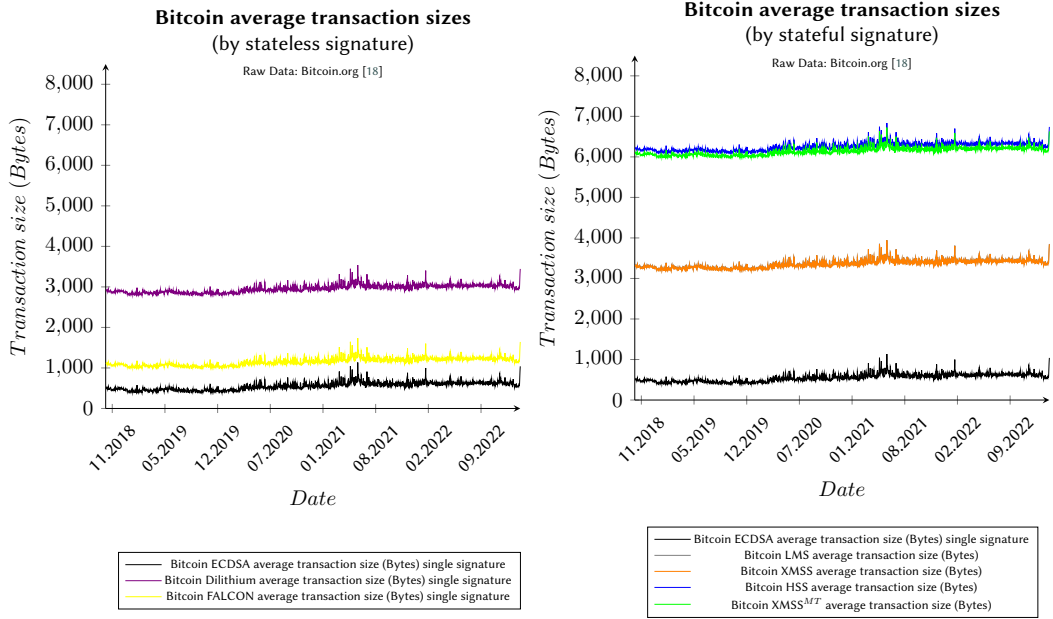


Figure 1: Signature impact on average transaction size

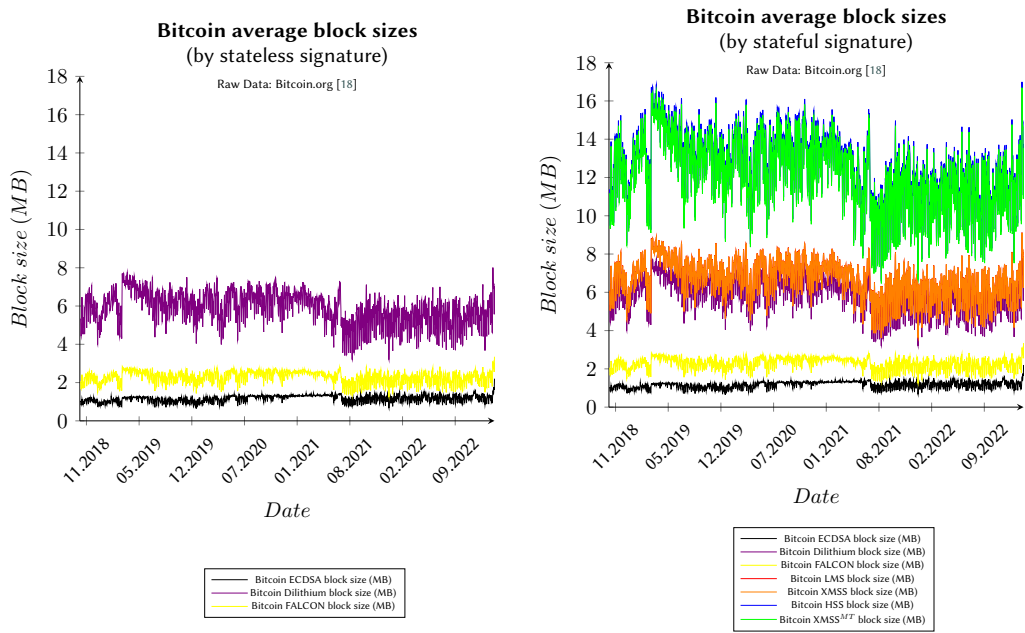


Figure 2: Signature impact on block size (MB)

see Figure 3. This illustrates the relative gap in transactions per block based on the adopted signature scheme. We summarise this in Table 1, which shows the comparison of post-quantum

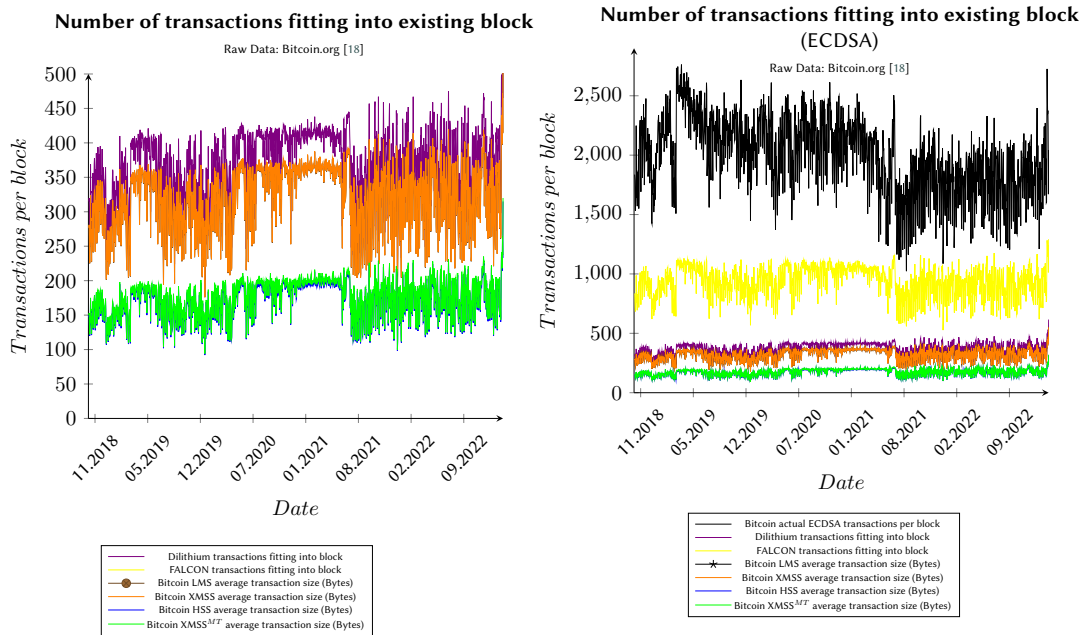


Figure 3: Number of transactions per 1MB block

signatures and the relative sizes of transactions, block size and number of transactions that fit into a 1 MB block.

For bitcoin, it is possible to reduce the block interval time (current target 10 minutes) to adapt to reduced transactions in a block. However, for other blockchains, with smaller block interval times, this option is not a practical solution. Ethereum, for example, has a 15 second block interval time target. Reducing this by a factor of 3 would make a target block interval time of 5 seconds, which would cause additional stresses on the performance of the blockchain.

3. Conclusion and further research

We have shown that the cost of using any of the NIST post-quantum finalist signature scheme candidates has a significantly negative effect on blockchain storage and communications costs. The FALCON stateless signature scheme offers the smallest signature scheme although it should be noted that the FALCON team are currently changing the scheme to address side channel attacks and the signature size is expected to increase. Stateful hash-based signatures offers smaller signatures and more transactions in a block and thus offer the most practical upgrade path at the cost of managing state in a dedicated wallet. Increasing the size of the block will improve the number of transactions per block. However, there are practical trade-offs in performance. For some blockchains, reducing the block interval time will be a possible solution. However, the best approach would be a new signature scheme that has characteristics similar to those of the current ECDSA signature scheme. NIST are currently running a competition for

smaller, more efficient signature schemes [19] and this research illustrates the need for such a scheme for blockchain and DLT systems.

We observe that the increased cost of adopting post-quantum signatures in blockchain and DLT systems supports the adoption of post-quantum layer-2 platforms to mitigate the cost and increase the transaction throughput of the blockchain and DLT system. However, most of the level-2 off-chain roll-up protocols today are not post-quantum safe, and both native layer-1 blockchain and layer-2 roll-up protocols will need to be post-quantum secure. As more valuable digital assets are tokenised, we also observe that it is likely that the security level requirement will increase. The NIST post-quantum signatures can offer higher security levels than today but at a significant additional cost in terms of signature sizes and signature key sizes impacting more negatively on the cost and performance for a blockchain or DLT system.

References

- [1] J. J. Kearneya, C. A. Perez-Delgado, Vulnerability of blockchain technologies to quantum attacks, arXiv preprint arXiv:2105.01815 1001 (2021) 1–10.
- [2] S. Holmes, L. Chen, Assessment of quantum threat to bitcoin and derived cryptocurrencies, Cryptology ePrint Archive, Report 2021/967 1001 (2021) 11–20.
- [3] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in: Proceedings of the 35th annual symposium on foundations of computer science, volume 999 of *CEUR Workshop Proceedings*, IEEE, 1994, pp. 124–134.
- [4] D. Cozzo, N. P. Smart, Sharing the luov: Threshold post-quantum signatures, <https://csrc.nist.gov/CSRC/media/Events/Post-Quantum-Cryptography-Standardization/documents/papers/session2-paper5-cozzo-presentation.pdf>, 2019.
- [5] U.S. National Institute of Standards and Technology (NIST), Pqc standardization process: Announcing four candidates to be standardized, plus fourth round candidates, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf>, 2022. Accessed 29 August 2022.
- [6] U.S. National Institute of Standards and Technology (NIST), Recommendation for stateful hash-based signature schemes, <https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>, 2020. Accessed on 7 February 2023.
- [7] U.S. National Institute of Standards and Technology (NIST), Post-quantum cryptography pqc security (evaluation criteria), [https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-\(evaluation-criteria\)](https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)), 2021. Accessed on October 16, 2021.
- [8] S. Bai, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé, Crystals-dilithium algorithm specifications and supporting documentation (version 3.1), pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf, 2021. Accessed on October 16, 2021.
- [9] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, Falcon: Fast fourier-lattice-based compact signatures over ntru, falcon-sign.info/falcon.pdf, 2021. Accessed 16th October 2021.

- [10] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, P. Schwabe, Z. Wilcox O’Hearn, Sphincs: practical stateless hash-based signatures, [sphincs.cr.yyp.to/sphincs-20141001.pdf](https://cr.yyp.to/sphincs-20141001.pdf), 2014. Accessed 16th October 2021.
- [11] N. Singh, M. Vardhan, Computing optimal block size for blockchain based applications with contradictory objectives, *Procedia Computer Science* 171 (2020) 1389–1398.
- [12] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, bitcoin.org/bitcoin.pdf, 2008. Accessed 7/10/2020.
- [13] V. Buterin, Ethereum white paper, whitepaper.io/document/5/ethereum-whitepaper, 2015. Accessed 30/10/2021.
- [14] M. Hearn, R. Gendal Brown, Corda: A distributed ledger, www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf, 2019. Accessed 30/10/2021.
- [15] H. foundation, An introduction to hyperledger, www.hyperledger.org/wp-content/uploads/2018/08/, 2019. Accessed 30/10/2021.
- [16] C. P. Schnorr, Efficient identification and signatures for smart cards, in: *Advances in Cryptology—Crypto ’89*, number 435 in *Lecture Notes in Computer Science*, Springer-Verlag, CEUR-WS.org, 1990, pp. 239–252.
- [17] C. P. Schnorr, Efficient signature generation by smart cards, *Journal of Cryptology* 4 (1991) 161–174.
- [18] Bitcoin.org, Block explorer, www.bitcoin.org, 2023. Created from downloading transactions as full bitcoin node.
- [19] U.S. National Institute of Standards and Technology (NIST), Call for additional digital signature schemes for the post-quantum cryptography standardization process, <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf>, 2022. Accessed 6 February 2023.