# REBOOTING THE WEB OF TRUST

**DESIGNING THE FUTURE OF DECENTRALIZED SELF-SOVEREIGN IDENTITY**

A RWOT VIRTUAL COMMUNITY PAPER

# *Quantum Secure DIDs*

by Dr. Carsten Stöcker (Spherity GmbH),
Dr. Samuel M. Smith (ProSapien LLC), and
Dr. Juan Caballero (Spherity GmbH)

**Keywords:** *decentralized identity, W3C DIDs, Digital Signatures, Key Rotation, Hash Functions, DAD, Key Event Receipt Logs (KERL), Key Event Receipt Infrastructure (KERI), Bitcoin P2PKH, Factorization, Hash Collisions, Quantum Computing, Cryptography*

**HOW TO MAKE A GIVEN DID METHOD POST QUANTUM SECURE WITH EXISTING CRYPTOGRAPHIC PRIMITIVES?**

## ABSTRACT

The cyberworld in which we spend our days — and upon which our lives depend — is built on weak security guarantees at the atomic level of the informational stack, and it is becoming more and more justified to question their longevity as building blocks. From nation-states trying to sway elections with fake news to ransomware that shuts down hospitals, we are living in a "Wild West" in which seemingly any data, or any transaction, may be compromised if interested parties devote enough resources to the attack. And like travellers in a lawless frontier, we are left to scan the horizon constantly for trouble, scrambling to plug the leaks in defences we cannot trust completely.

We are vulnerable not just to sophisticated social engineering techniques, but also to the increasing sophistication of a rapidly professionalizing workforce of full-time cybercrime mercenaries, who are today as likely to work for well-funded criminal organizations or governments as be free agents working for their own interests [21]. Now even greater risk will materialize from the development of new offensive tools such as quantum computers, which might soon be powerful enough to crack many of today's most widely used cryptographic ciphers.

Today's best publically-available security standards and practices are based on our (over)confidence in the math underlying our existing cryptographic primitives. These are nevertheless still inherently vulnerable to a mind like that of Alan Turing, whose critical approach proved decisive in breaking the German Enigma code in World War II [1]. Unfortunately, it is not a matter of public record how many enterprises or governments are investing substantially in research to develop special-purpose computers engineered to break existing ciphers, be they quantum computers or otherwise. Since such projects are inherently a matter of national security, and easily hidden from public scrutiny, we cannot know their number, their scale, or how close they are to working results. When such quantum computers become available (in years or even months), our digital identity systems will be significantly more vulnerable than they are now. We cannot assume we will have any prior warning to change course once such cryptographic lockpicks start being deployable, or that we will even have certainty that this epochal shift has taken place after they start to be deployed.

Decentralized identity systems are particularly vulnerable to such cryptographic attacks since the granular proliferation of local keys that rids the world of honeypots also makes it so hard to detect if individual keys start to be compromised on a small scale. To address the risk represented by the advent of quantum computing for decentralized identity solutions, we propose to introduce a simple method using one-time signing keys and key rotation to protect our digital identity while using existing cryptographic ciphers for signing and hashing. This method will allow us to forge a mitigation strategy today for the coming age of "quantum attacks" on our otherwise secure identity systems based on public key cryptography.

The objective of this paper is to describe a mechanism for protecting DIDs using existing ciphers for signing during the transition phase to a fully quantum-secure decentralised identity infrastructure. This mechanism is designed to support DIDs but its core mechanisms are identifier-independent and DID:method-independent. Analysis of secure key-management solutions for multiple keys and quantum-resistant ciphers for signing are

beyond the scope of this paper and assumed to progress in parallel. This paper describes a quantum-resistant architecture for today's non-quantum-resistant ciphers*, intended to be retrofitted to existing systems.

## BACKGROUND: MOTIVATION FOR OUR WORK

When practical quantum computing finally arrives, it will likely power ways to crack the standard cryptographic ciphers for signing and encryption that safeguard our online privacy. The goal of quantum-computer engineering is to directly build qubits as physical devices that can efficiently and reliably carry out quantum operations. The theory behind "quantum error correction" implies the threshold of reliability required for quantum computing to be useful may be quite low.

Currently intractable computational problems that protect widely-deployed cryptosystems, such as RSA and Elliptic Curve-based schemes, are expected to become solvable in the post quantum age. This is why NIST has challenged researchers to develop a new generation of quantum-resistant cryptographic algorithms [2].

Many experts don't expect a quantum computer capable of performing the complex calculations required to crack modern cryptography standards to become a reality within the next 5 to 10 years [3]. On the less optimistic side, however, very little information is public about the special-purpose quantum developments being researched in government-funded research projects in Beijing, Fort Meade, Cheltenham, Langley, Moscow, Pyongyang, or Tehran. The timeline of quantum cryptography is thus highly unpredictable. Likewise, consensus around the level of security risk (and thus, large-scale investment in systems it endangers) remains elusive.

As so much is at stake, from personal safety and enterprise security to our civil order, the cryptography community is working on quantum-resistant ciphers [4] [5]. The RWoT community needs to be prepared by getting solutions in place to protect the decentralized identity instruments we are all currently working on.

## PRIOR ART: COST ANALYSIS OF FACTORIZATION AND HASH COLLISIONS USING QUANTUM COMPUTERS

Public-key cryptography has not only been at the centre of internet communication and online transactions for decades, it is also at the centre of RWoT's decentralized identity work. With computing power growing at an exponential rate, however, some of the most widely used encryption schemes are starting to show their limits. This section will review some recent research to offer non-controversial starting points for which kinds of existing cryptography can be judged particularly vulnerable to quantum attacks and which existing technologies can be used to replace them.

Decentralized identity implementations often depend on a security model that makes the computing power required to brute-force or deduce a private key sharply asymmetrical to the computing power required to use it on conventional computing architecture. For example, popular primitives such as ECDSA or Schnorr are considered very strong based upon the intractability of certain discrete-logarithm problems, which require implausibly vast computing resource to attack with today's computer architectures.

Some primitives, such as elliptic-curve cryptography, are more vulnerable to attacks by quantum computers than others. In the classical case, the most efficient algorithms have purely exponential running time. In the quantum case, however, there exists a variant of Shor's algorithm that can solve the elliptic-curve discrete-logarithm problem through factorization in polynomial time [6].

Our paper is founded on the research of Daniel J. Bernstein and his work on the cost analysis of factorization and hash collisions using quantum computers [7]. It is based on the following conclusions of his work:

1. Quantum computers will be much more scalable than number-factorization hardware, and therefore much more cost effective for assembling massive compute resources than number-factorization hardware.
2. All known quantum algorithms are less cost effective than traditional cryptoanalytic hardware when it comes to finding collisions in hash functions, even under optimistic assumptions regarding the speed of quantum hardware.
3. Quantum computers will likely be far more efficient when used for sufficiently large factorizations, but they may never be as efficient when used to run collision searches.

These theoretical conclusions do not depend on the engineering difficulty of building quantum computers; they will remain true even in a world full of mature and stable quantum computers. Within the space of known quantum-collision algorithms, the most cost-effective algorithms are equivalent to non-quantum algorithms. Hash collision algorithms should thus be implemented with standard bits rather than with qubits.

> *If hash algorithms can be considered secure with regards to classical computing, they can be considered secure in the post-quantum area as well.*

The current best practice is that 128 bits of cryptographic strength is sufficient for the near future, and our research supports the conclusion that this may be extended to include post-quantum cryptographic strength. Algorithms that maintain 128 bits of strength post-quantum are also sufficient for the near future. Consequently, we consider one-way hash functions such as Blake2-256 or greater, Blake3-256 or greater, SHA3-256 or greater, and SHA2-512 to be both pre- and post-quantum secure because they maintain at least 128 bits of cryptographic strength post-quantum.

### INSPIRATION FROM BITCOIN

Since Google announced that it had achieved quantum supremacy [8], the topic of security for cryptographic systems in general and for Bitcoin in particular is being picked up in a broader public debate [9]. Bitcoin offers multiple address schemes for peer-to-peer transactions of which we compare two because of their relevance to quantum resistance:

Pay to public key (p2pk): This address type was the first instrument programmed into Satoshi's BTC protocol. Since all transactions are public, anyone could obtain the public key from the ledger and solve its factorization problem with a sufficiently powerful quantum computer, thus discovering the corresponding private key, which could be used to unlock a BTC wallet.

Pay to public key hash (p2pkh): The address of the recipient’s wallet is derived from a one-way hash-function of the public key. The public key is not directly revealed by the address: it will only be revealed for the first time if the recipient signs and initiates a BTC transaction. This means that if BTCs have never been transferred from a p2pkh-blinded address, the public key has not been published to the ledger, and the private key cannot be derived using a quantum computer. When BTCs are transferred for the first time, the public key is revealed and the wallet cannot be considered quantum-secure any more.

An unused BTC p2pkh address can be considered quantum secure (i.e., it is impossible or many, many orders of magnitude harder – and therefore practically impossible – to derive the private key from a public key one-way hash compared with a situation where the public key is directly exposed). As long as I have a wallet that was never used to transact BTC, a malicious actor cannot derive my private key, even with access to a theoretical quantum computer infrastructure powerful enough to calculate private from public keys.

## MAKING DID METHODS AND ARCHITECTURES QUANTUM-SECURE BY DESIGN

Like BTC, Ethereum adopted the one-way hash function approach for creating an Ethereum Wallet address; Ethereum's DID method, DID:ethr, benefits from this blinding mechanism. Similar approaches are also adopted by other DID methods such as Sovrin's DID:sov.

Using the Ethereum lightweight identity standard ERC-1056, a default (un-configured) DID document can be considered quantum secure. But when the DID document is first configured, a blockchain transaction is signed and the public key is revealed. Unless the public key is deactivated by rotation, the DID document cannot be considered post quantum secure any more. Normative guidance and/or a change of syntax at the ERC/Ethereum-core level may be justified to prevent entire systems automating this vulnerability into identity systems.

But the above only covers DID operations; Verified Credential issuance necessarily entails revealing a public key, at least to the holder of the credential. The public signing key in most DID systems is exposed when issuing a verifiable credential or signing a verifiable presentation. Reconceiving PKI infrastructure to minimize public key exposure would add significant complexity to SSI systems.

DID C.R.U.D. mechanisms generally rely on the cryptographic primitives of the underlying DID method and DLT implementation (e.g. ECDSA in case of Ethereum). A malicious actor enabled by quantum computing could take control of a DID document by using the public-key information. We could therefore consider the corresponding private key to be insecure *per se* in a post quantum world in either case (VC issuance or CRUD), regardless of whether signing happens on-chain or off-chain.

In order to mitigate a theoretical quantum-computing attack, we propose the following measures:

- To register one-way hashed public keys rather than clear public keys as authorization attributes for all DID document operations, and
- To simultaneously deactivate and/or rotate the public key hash used every time the respective public key is exposed either in on-chain or off-chain signing processes.

To enable a quantum-secure DID method we propose to apply key rotation mechanisms after each on-chain or off-chain signing transaction. This approach is independent of the DID method implementation, although clearly this could be a massive blow to the simplicity or cost effectiveness of blockchain-dependent methods. Key rotations events could be moved off of the blockchain (or other public oracle) used to publish DIDs at their genesis with some kind of alternate, more local consensus system for the maintenance of key material state, such as a system like KERI (key-event receipt infrastructure), which creates verifiable linked logs of key rotation events over time [10]. In this way, DID systems can maintain state and chronology of public keys in a more efficient and lightweight parallel system than the public oracle they use to vouchsafe the age and existence of each DID, whose DID documents they still already have to be trusted to resolve.

Crucially, KERI or any other such "parallel"/off-chain key state mechanism could be maintained and queried without reference to block confirmation times on a blockchain. Since such a system does not need its chronology to be precisely lockstepped to the chronology of the blockchain, there is no reason to bottleneck its efficiency or complexity just to benefit from the consensus underlying its infrastructure. Such systems are therefore a promising building block for making DID systems quantum secure, since they can trigger a lightweight key rotation event every time a verifiable credential / presentation signing transaction necessitates one, without requiring a blockchain operation.

## RECIPE FOR POST-QUANTUM SECURE DIDS

Our proposed recipe for making DIDs quantum-secure with existing cryptographic ciphers is based on the following user journeys:

### A. Initializing a new DID

As a user of DIDs and a new holder of a DID of which I am the subject or subject's guardian, I would like to initialize a new DID from high-quality entropy by performing the following steps:

1. Generate initial public/private key-pair from high-quality randomness, preferably using a quantum random number generator (QRND [11]), and use that keypair to derive the DID identifier through a secure one-way hash function (e.g., SHA2-512 in multihash format).
2. Generate **keypair tuples** for signing on behalf of the DID and performing key rotation operations.
3. Create and configure the genesis DID document and/or genesis key event log entry while simultaneously configuring one or more **public keypair tuples hashes** to put in it/them

**B. Signing Operations**

As a user of DIDs and a holder of a DID's controlling private key, I would like to sign a transaction, credential, or presentation and I do not want to be vulnerable to a quantum attack leveraging the disclosed public key. I should:

1. Sign DID-document or verifiable credential / presentation transactions with private key #1 of my current keypair tuple
2. Simultaneously use key #2 from the same keypair tuple to sign a key rotation transaction, thus deactivating the entire keypair tuple whose hashes have been public until now

Notes:

- In the case of a DID-document transaction, the DID-document update and key rotation transactions can be signed with the same private key; the multiplication of related keys is simply a protection against unwanted correlation of steps B1 & B2.
- In the case of a DID holder running out of unused key pair tuples for a given DID subject identifier, the holder might need to deactivate public keypair tuples hashes and to register new keypair tuple hashes at the same time.
- Simultaneous signing of credential (or presentation) issuance and key deactivation (or rotation) requires precision synchronization among the signing transactions and the issuing time stored in the credential (or presentation). Timing and security parameters should be considered with reference to the response times of the key rotation methods as well as the time needed to retrieve a private key from a public key through attack with a quantum computer. Setting tolerances for synchronization thus requires balancing attack risk against implementation cost and complexity.
- The mechanism described here is entirely feasible today as modelled on today's DID systems and a reference implementation of KERI according to its current design; both elements are, of course, being iterated and growing more complex over time.

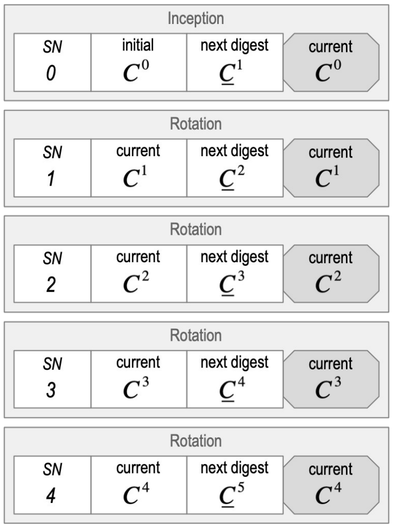
**C. Verifying a Credential**

As an inspector of credentials, I would like to verify a verifiable credential or presentation. I should: 1. Verify the expiration and the revocation information in accordance to the W3C standards and a relevant revocation method 1. Verify the issuing time of the credential as well as the validity and deactivation time of the public key hash in the DID document and/or KERI event log

**KERI APPROACH**

KERI uses a pre-rotation scheme in each rotation event that also makes a forward cryptographic commitment to the next rotation key or set of keys [18][19]. Pre-rotation is an elegant way of managing rotation keys. With pre-rotation, a given rotation key set can only be used once. If this forward commitment is expressed as a digest of the next rotation key set, then the pre-rotation can be considered post-quantum secure. The latest version of the

KERI design white paper proposes this approach. Details of this scheme can be found here [20]. The nearby diagram shows the basic idea of pre-rotation with post-quantum secure digests of the next key sets.



**CONCLUSION**

Quantum computers far outperform conventional computers when faced with sufficiently large factorizations, but they do not outform on collision searches. Therefore, existing cryptographic primitives for signing can be considered as vulnerable to quantum attacks. Hashing algorithms can be considered as resilient against quantum attacks. This uneven distribution of vulnerabilities allow us to design methods for making DIDs much more quantum-secure while using existing cryptographic primitives. This approach can be considered for use in the transition period from existing ciphers being potentially vulnerable to quantum factorization to quantum resistant ciphers becoming avialable for signing.

In particular, the KERI design allows cryptographically verifiable and highly efficient key deactivation and rotation operations. We propose considering a more rotation-intensive paradigm for DIDs, particularly high-stakes DIDs like those used for natural person and legal person identities, as one method of quantum-proofing SSI infrastructure as whole. It may well make sense to refine and publicize the proposed method for enabling post-quantum secure DIDs as a standard mechanism as a non-normative addendum to a KERI reference implementation, when that is published.

A more generic, standard definition might some day be worth considered for a future iteration of W3C DID working group.

**References**

[1] Wikipedia, Alan Turing, https://en.wikipedia.org/wiki/Alan_Turing

[2] NIST, G. Alagic et al, 01/2019, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf

[3] IEEE Spectrum, J. Hsu, 09/2019, How the United States Is Developing Post-Quantum Cryptography, https://spectrum.ieee.org/tech-talk/telecom/security/how-the-us-is-preparing-for-quantum-computings-threat-to-end-secrecy

[4] MIT, J. Wohlwend, 2016, Elliptic Curve Cryptography: Pre and Post Quantum, https://math.mit.edu/~apost/courses/18.204-2016/18.204_Jeremy_Wohlwend_final_paper.pdf

[5] Fraunhofer, R. Niederhagen et al, 10/2017, Practical Post-Quantum Cryptography, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Practical.PostQuantum.Cryptography_WP_FraunhoferSIT.pdf?_=1503992279

[6] Cornell University, C. Zalka, 1998, Fast versions of Shor's quantum factoring algorithm, http://arxiv.org/abs/quant-ph/9806084

[7] University of Illinois at Chicago, Daniel J. Bernstein, 08/2009, Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?, https://cr.yp.to/hash/collisioncost-20090823.pdf

[8] Google, John Martinis et al, 10/2019, Quantum Supremacy Using a Programmable Superconducting Processor, https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

[8] Deloitte, I. Barmes et al, 2019 Quantum computers and the Bitcoin blockchain https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html

[9] Bitcoin Wiki, Bitcoin Address, https://en.bitcoin.it/wiki/Address

[10] Cornell University, S. Smith, 07/2019, Key Event Receipt Infrastructure (KERI), https://arxiv.org/ftp/arxiv/papers/1907/1907.02143.pdf

[11] Medium, C. Stöcker et al, 09/2017, Randomness: The Fix for Today's Broken Security, https://medium.com/@cstoecker/randomness-the-fix-for-todays-broken-security-39ea7dc3a89b

[12] "Blake3," Github, https://github.com/BLAKE3-team/BLAKE3

[13] "BLAKE3 Is an Extremely Fast, Parallel Cryptographic Hash," InfoQ, 2020/01/12 https://www.infoq.com/news/2020/01/blake3-fast-crypto-hash/

[14] Unruh, D., "Collapsing sponges: Post-quantum security of the sponge construction," IACR, 2017/03/27 https://eprint.iacr.org/2017/282.pdf

[15] Saarinen, M.-J. and Aumasson, J.-P., "The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC) IETF RFC-7693," IETF RFC-7693, 2015/11/01 https://tools.ietf.org/html/rfc7693

[16] "BLAKE2 — fast secure hashing," Blake2, https://blake2.net

[17] "What security do Cryptographic Sponges offer against generic quantum attacks?," Crypto StackExchange, 2019/08/01 https://crypto.stackexchange.com/questions/419/what-security-do-cryptographic-sponges-offer-against-generic-quantum-attacks?rq=1

[18] Smith, S. M., "Decentralized Autonomic Data (DAD) and the three R's of Key Management," Rebooting the Web of Trust RWOT 6, Spring 2018. https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/DecentralizedAutonomicData.pdf

[19] Smith, S. M., "Key Event Receipt Infrastructure (KERI) Design and Build," arXiv, 2019/07/03 https://arxiv.org/abs/1907.02143

[20] Smith, S. M., "Key Event Receipt Infrastructure (KERI) Design," Github, 2020/04/22 https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

[21] Hilary, Gilles, and Durand, Christoph, "The Professionalisation of Cyber Criminals," April 11, 2016 https://knowledge.insead.edu/blog/insead-blog/the-professionalisation-of-cyber-criminals-4626)

**Additional Credits:**

**Authors:** Dr. Carsten Stöcker (Spherity GmbH), Dr. Samuel M. Smith (ProSapien LLC)

**Editor & Co-Author:** Dr. Juan Caballero (Spherity GmbH)

**Sample APA Citation:**

Stöcker, C., Smith, S., and Caballero, J. (2020). Quantum Secure DIDs. *Rebooting the Web of Trust Virtual*. Retrieved from https://github.com/WebOfTrustInfo/rwot10-buenosaires/blob/master/final-documents/quantum-secure-dids.pdf.

**About Rebooting the Web of Trust**

*This paper was a virtual collaboration based on a topic originally intended for the Rebooting the Web of Trust X design workshop, which was cancelled due to COVID-19. The credit goes to our community, who continues to work together even as we shelter in place.*

**RWOT Board of Directors:** Christopher Allen, Joe Andrieu, Kim Hamilton Duffy

**Members of the Organizing Committee:** Dan Burnett, Dmitri Zagidulin

**Community Sponsors:** Blockchain Commons, Consensys, Learning Machine, Legendary Requirements

**Workshop Credits:** Christopher Allen (Founder, Co-Producer), Joe Andrieu (Co-Producer and Facilitator), and Shannon Appelcline (Editor-in-chief).

*Thanks to our other contributors and sponsors!*

**What's Next?**

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rwot9/issues

We hope to run an eleventh Rebooting the Web of Trust design workshop as long term solutions emerge for the COVID-19 pandemic. If you'd like to be involved or would like to help sponsor the event, email:

rwot-leadership@googlegroups.com