Journal of Psychology and AI

ISSN: 2997-4100 (Online) Journal homepage: www.tandfonline.com/journals/tpai20

Quantum-resistant timestamping for open science: a non-technical guide

Christian U. Krägeloh, Emerson J. Bartholomew & Oleg N. Medvedev

To cite this article: Christian U. Krägeloh, Emerson J. Bartholomew & Oleg N. Medvedev (2026) Quantum-resistant timestamping for open science: a non-technical guide, Journal of Psychology and AI, 2:1, 2639409, DOI: 10.1080/29974100.2026.2639409

To link to this article: https://doi.org/10.1080/29974100.2026.2639409

Published online: 16 Mar 2026.

JOURNAL OF PSYCHOLOGY AND AI
2026, VOL. 2, NO. 1, 2639409
https://doi.org/10.1080/29974100.2026.2639409

Taylor & Francis
Taylor & Francis Group

METHOD

OPEN ACCESS Check for updates

Quantum-resistant timestamping for open science: a non-technical guide

Christian U. Krägeloh [a], Emerson J. Bartholomew [b] and Oleg N. Medvedev [c]

[a]Department of Psychology and Neuroscience, School of Science, Auckland University of Technology, Auckland, New Zealand; [b]Department of Psychological Medicine, University of Auckland, Auckland, New Zealand; [c]School of Psychology, University of Waikato, Hamilton, New Zealand

ABSTRACT

Psychology faces a dual challenge from artificial intelligence (AI): While AI offers powerful research tools, it simultaneously threatens the discipline's methodological foundations through deepfakes and synthetic data generation. The ability to prove when psychological data, preregistrations, and research protocols genuinely existed has become critical for maintaining scientific integrity, particularly as AI can now fabricate convincing retroactive evidence. These concerns are compounded by the vulnerability of existing open-science platforms to cyberattacks, data loss, or service unavailability, raising broader questions about the reliability and security of current research infrastructure. Together, these threats make robust, independent verification of research records increasingly urgent, especially in the context of psychology's ongoing replication crisis and open-science reforms. This method article presents a quantum-resistant blockchain timestamping solution for researchers with no technical blockchain knowledge. Using the example of the Algorand blockchain's Falcon cryptographic signatures – which are understood as being able to withstand both current AI threats and future quantum-computing attacks – we are demonstrating how researchers can create immutable proof that their hypotheses, data collection protocols, and datasets existed at specific times at the cost of a fraction of cent. Through step-by-step instructions, this article enables researchers to implement quantum-resistant timestamping regardless of their technical background. By removing barriers to blockchain-based verification, this method aims to make such protection as routine as current preregistration practices, ultimately establishing a new standard for safeguarding research integrity in the age of AI.

ARTICLE HISTORY
Received 2 October 2025
Accepted 25 February 2026

KEYWORDS
Blockchain timestamping; research integrity; quantum-resistant cryptography; preregistration; open science

1. Introduction

The importance of replication in psychological research has been a central concern for decades, with ongoing debates about research reproducibility spanning from earlier methodological critiques (Schmidt, 2009) to regular calls for awareness of the contemporary replicability crisis (Maxwell et al., 2015), including recent reminders (Bogdan, 2025; Nosek et al., 2022). Other work has conducted surveys about researcher awareness of the issue (Baker, 2016) and even attempted to estimate the extent of the reproducibility problem in psychological science (Open Science Collaboration, 2015).

This sustained attention has coincided with a gradual cultural shift towards open-science practices, supported by recognised guidelines (Munafò et al., 2017). Recent meta-research indicates moderate but meaningful progress in adoption of these practices in psychology: Field-wide estimates indicated that preregistration increased from approximately 3% in 2014–2017 to 7% by 2022, while open raw data availability rose from roughly 2% to 14% over the same period (Hardwicke et al., 2022, 2024). By contrast, longitudinal full-text analyses of empirical articles ($n = 15{,}634$) in six leading psychology journals revealed that these practices were virtually absent between 2004 and 2012, but increased sharply thereafter, such that by 2024 approximately 40% of articles reported preregistration and 73% provided open data (Pfadt et al., 2025).

As Banks et al. (2019) comprehensively outlined, open science encompasses diverse practices including data sharing to improve reproducibility, preregistering studies to distinguish between confirmatory and exploratory research, and engaging in replication studies to assess generalisability. The movement has gained particular momentum following concerns that standard research practices undermine fundamental

CONTACT Christian U. Krägeloh chris.krageloh@aut.ac.nz

scientific principles (Crüwell et al., 2019). As Hesse (2018) noted, open science fundamentally refers to "the social and epistemological movement – enabled by the tools of the information age – to make the publication of scientific concepts together with the protocols and data upon which those concepts are based readily accessible to all levels of an inquiring society" (p. 126).

However, just as the field has made substantial progress in establishing these open-science norms, emerging technologies present new challenges to research integrity. The rapid advancement of artificial intelligence (AI) capabilities, particularly in generating synthetic data and creating sophisticated deepfakes, introduces unprecedented threats to the verifiability of research materials. As Doss et al. (2023) demonstrated already some time ago, between 27% and 50% of education stakeholders cannot distinguish authentic videos from deepfakes – and technology is continuously improving. Galyashina and Nikishin (2022) specifically warned that voice deepfakes pose particular dangers to scientific communication, as they can fabricate "pseudo-real information and communication events" that threaten the credibility of research infrastructure. The emergence of generative neural networks and other AI technologies has dramatically lowered the barriers to creating manipulated digital content that appears authentic (Doss et al., 2023). Researchers now face the dual challenge of demonstrating not only that their data and preregistrations exist in specific forms, but also that these materials existed at particular times – crucially, before data collection, before seeing results, or before similar findings were published elsewhere – as deepfake technologies make it increasingly possible to fabricate evidence retroactively.

The importance of timestamping of research files can be illustrated through documented cases of scientific fraud. In one of psychology's most prominent misconduct cases, social psychologist Diederik Stapel was found to have fabricated data across dozens of publications over many years. Formal investigation committees reported that the original datasets were frequently unavailable, incomplete, or unusable, and that for entire subsets of publications no original data could be recovered at all – severely limiting retrospective verification of integrity (Levelt et al., 2012). More broadly, large-scale analyses of retracted articles in psychology indicate that scientific misconduct is neither rare nor easily detected, and that the most common forms of misconduct involve the fabrication, falsification, or manipulation of research datasets (Craig et al., 2020). Meta-analytic evidence estimates that approximately 2.9% of researchers self-report having committed at least one instance of fabrication, falsification, or plagiarism, while 15.5% report having witnessed such misconduct by others (Xie et al., 2021), with witness-reported rates in biomedical research being considerably higher at 27.9% for plagiarism and 33.6% for data falsification (Phogat et al., 2023). Investigations of scientific misconduct are typically initiated by whistleblowers or by suspicions arising from post-hoc anomalies in published results, including the unavailability of original datasets, rather than through systematic verification mechanisms (National Academies of Sciences, Engineering, and Medicine, 2017; Stroebe et al., 2012).

Blockchain technology – the distributed ledger system that underlies cryptocurrencies like Bitcoin – offers a promising solution to this temporal verification problem (Dong et al., 2023). A distributed ledger can be understood as a shared digital record book that is replicated across many independent computers, where new entries are added sequentially and permanently rather than edited or overwritten. While blockchain is often associated with digital currencies, its core innovation lies in creating permanent, tamper-proof records that multiple parties can verify independently. When applied to research verification, this technology enables what is known as blockchain-based timestamping. Early work by Gipp et al. (2017) demonstrated how blockchain-based timestamping could be used to establish priority and verify the existence of scholarly manuscripts and related research artefacts independently of repositories or submission platforms. Wittek et al. (2020) extended earlier blockchain-based timestamping approaches by integrating cryptographic proof-of-existence services into the bloxberg research blockchain, with a focus on usability and workflow integration. By generating a unique cryptographic hash – essentially a digital fingerprint – of any file and storing this hash on a blockchain ledger, researchers can create proof that their preregistrations, data, or analysis plans existed in exact forms at precise moments. Taken together, these approaches have immediate applications for verifying preregistration timing, establishing priority for discoveries, and protecting against risks such as data leakage, reviewer misconduct, and post-hoc modifications of research protocols and datasets.

Current open-science infrastructure appears insufficiently equipped for an evolving landscape of technology-related threats. Platforms such as the Open Science Framework were designed to promote

transparency, accessibility, and reproducibility rather than to provide cryptographically immutable records. As practical guides to open research workflows describe, records on platforms such as the Open Science Framework rely on platform-generated timestamps and read-only registrations to document study plans (Klein et al., 2018). These mechanisms support transparency within established research infrastructures but do not provide cryptographic, third-party-verifiable proof of the existence of a specific digital state at a given time. Repository timestamps and version histories document uploads and modifications within the platform's own system. While this supports transparency under normal operating conditions, verification ultimately depends on trust in the platform's integrity and continued operation. These mechanisms do not generate externally anchored cryptographic proofs that can be independently verified outside the platform's infrastructure in adversarial contexts. Such platforms have experienced serious issues with spam, thus threatening their security (Cohoon, 2024a). Documented analyses have also shown that open science platforms, including the Open Science Framework, have been actively exploited for piracy, phishing, and other malicious activities (Ikeda et al., 2023). Open-science infrastructures may also be increasingly vulnerable to misappropriation and AI-enabled disinformation. This is partly because their design emphasises inclusivity and low barriers to participation, often involving minimal user credentialing, which can expose these systems to misuse and security threats (Cohoon, 2024b).

The alteration or forgery of timestamps, or *timestomping*, has become a common technique to hide evidence or obstruct investigations (Palmbach & Breitinger, 2020). Such manipulation is technically straightforward and difficult to detect retrospectively using conventional forensic artefacts (Palmbach & Breitinger, 2020), highlighting the limitations of verification approaches that rely solely on file system metadata rather than cryptographic proof. These considerations underscore why blockchain-based systems have been proposed to provide what Boetto et al. (2021) termed a "license of reliability" for research studies – enabling independent verification of when data existed and whether it has been altered, without dependence on trust in any single institution or platform.

To illustrate, consider a researcher who preregisters a study on an open-science platform. The timestamp on that preregistration depends on the platform's servers accurately recording and preserving the date. If the platform's infrastructure were compromised – whether through a cyberattack, a technical failure, or administrative error – there would be no independent means of verifying when the document was originally uploaded. By contrast, if the researcher had also generated an SHA-256 hash of the preregistration file and stored it on a blockchain, this creates a verification record that exists independently of any single platform. Even if the original platform were to become unavailable or its records were disputed, anyone with the original file could recompute the hash and confirm it matches the blockchain record, thereby independently verifying the document's existence at that time. Blockchain timestamping thus provides a complementary, independent layer of verification rather than a replacement for existing open-science platforms.

Yet, even as blockchain timestamping addresses current verification needs, a new technological challenge looms on the horizon. The development of quantum computing threatens to undermine the cryptographic foundations of most existing blockchain systems. Unlike classical computers that process information as binary bits (either 0 or 1), quantum computers exploit quantum mechanical properties such as superposition – allowing quantum bits or *qubits* to exist in multiple states simultaneously – enabling them to solve certain mathematical problems exponentially faster than conventional computers (Gill et al., 2022). Quantum computers, once sufficiently advanced, could potentially break the encryption algorithms that current blockchains rely upon for security (Fernández-Caramés & Fraga-Lamas, 2020), rendering existing timestamps vulnerable to manipulation or forgery. In practical terms, most current blockchain systems secure their records using mathematical problems that are extremely difficult for classical computers to solve – for example, deriving a private cryptographic key from a public one. A sufficiently powerful quantum computer could solve such problems rapidly, potentially allowing an attacker to forge the digital signatures that guarantee the authenticity and immutability of blockchain records.

The present method paper introduces a quantum-resistant timestamping method using the Algorand blockchain, a fast and secure blockchain system that confirms transactions using a Pure Proof-of-Stake consensus mechanism rather than the computational mining used by traditional blockchains (Divya & Uma Priyadarsini, 2025). Algorand employs Falcon cryptographic signatures designed to withstand quantum-

computing attacks (Allende et al., 2023; Gandhi et al., 2024; Zhaolu et al., 2025). Falcon cryptographic signatures are a type of digital signature used to authenticate transactions and protect them against tampering. Unlike many traditional signature schemes currently used in blockchains, which are vulnerable to future quantum-computing attacks, Falcon was specifically designed to remain secure in a post-quantum setting (Zhaolu et al., 2025). Accordingly, Algorand's architecture provides long-term security for research timestamps while remaining accessible to researchers without blockchain expertise. We present a non-technical, step-by-step method that requires no cryptocurrency trading or specialist blockchain knowledge, enabling any researcher to create permanent, quantum-resistant proof of their research materials' existence at specific points in time.

In essence, this method allows researchers to generate a short string of characters that uniquely represents their file's content and store this information on the Algorand blockchain, where it becomes part of an unchangeable, permanent record. This simple process, which is detailed in the following sections, provides researchers with a powerful tool for ensuring the temporal integrity of their work in an era of advancing technological threats. Importantly, open-science practices need to come with minimal costs (Hales et al., 2019), and this method is intended to highlight an avenue of cost-effective timestamping of research documents.

2. Method

The timestamping process involves three steps:

(1) computing an immutable digital fingerprint (hash) of your research artefact (e.g. PDF document)
(2) storing this hash as a transaction note on a blockchain
(3) recording the transaction ID and making it publicly available to enable later verification.

Choosing a quantum-resistant blockchain such as Algorand ensures the hash (and thus proof of your document's existence) cannot be altered retroactively, even by using quantum computing.

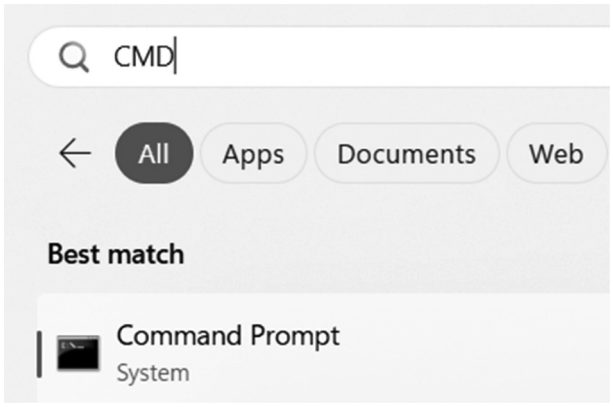
2.1. Step 1: computing a hash of your research document

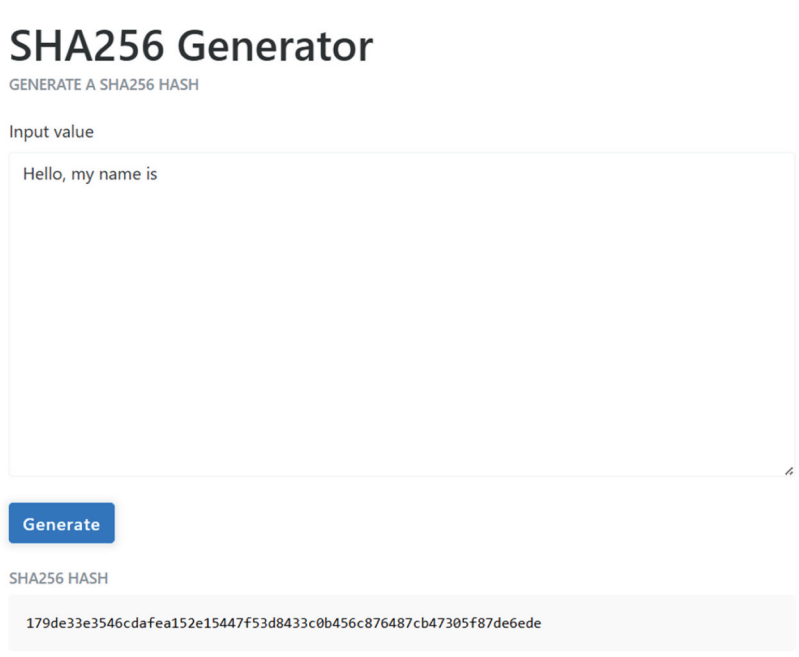
To timestamp a research document such as a preregistration file (e.g. a PDF) or a dataset (e.g. an Excel spreadsheet), the first step is to generate a cryptographic hash. A hash is essentially a unique digital fingerprint – a fixed-length string of characters that serves as a distinctive identifier for your specific file. This code is mathematically derived from the document's exact binary content using a one-way algorithm, meaning that, while any file can be converted to a hash, the original file cannot be reconstructed from the hash alone.

The uniqueness of hashes is fundamental to their utility. While numerous cryptographic hash functions are available, including SHA2, Keccak, SHAVITE, and Blake (Kuznetsov et al., 2023), SHA-256 is commonly used as it provides an optimal balance of security and computational efficiency. With a 256-bit output, SHA-256 can generate 2^{256} unique hashes, representing an extremely large number of possible values. This makes a "collision", where two different files produce the same hash, highly unlikely (Selvakumar & Ganandhas, 2009).

Hashing can be carried out in different ways. The simplest way is to create a hash on one of the many hash generator websites (such as https://tools.keycdn.com/sha256-online-generator). One can easily see how small changes can result in completely different hashes, such as when comparing the top and bottom panels of Figure 1.

In the example shown in Figure 1, hashes had been generated from simple text. However, hashes can also be calculated for entire files, including very large datasets. For brevity, we only outline a method to create a hash for a file using a Windows computer. After clicking the "Windows" key on the keyboard, type "CMD" in the search field:





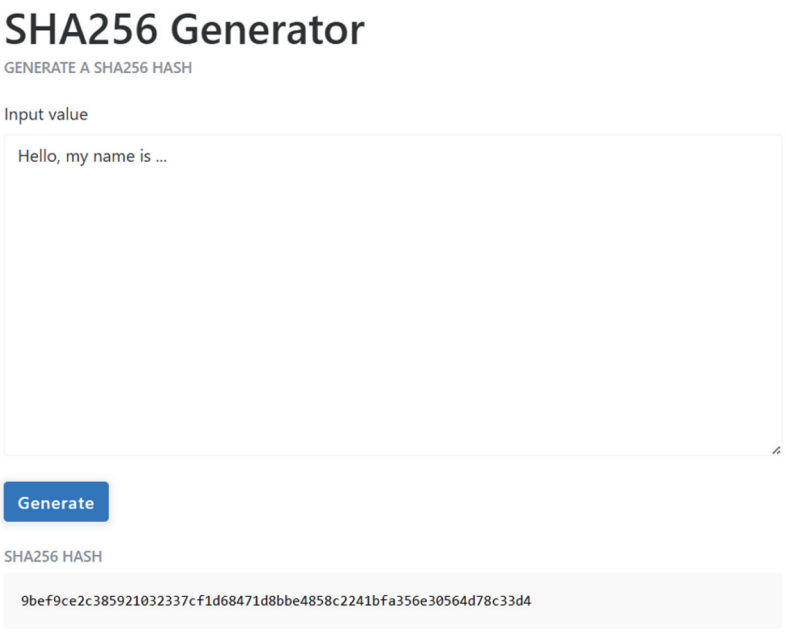
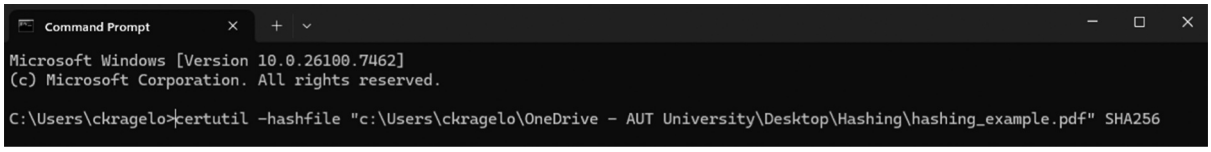


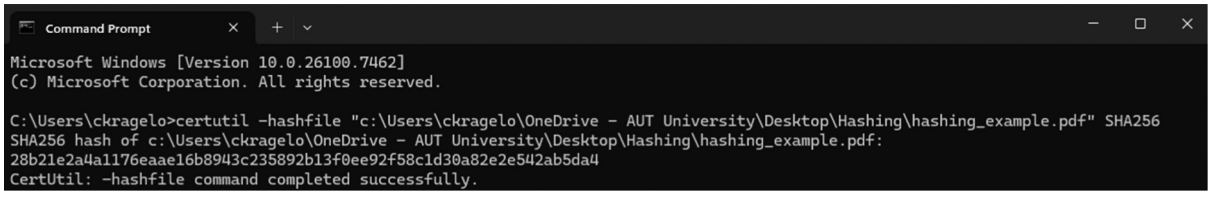
Figure 1. Hashes generated on an online website, based on simple text. A small variation of the text (bottom panel) results in a completely different SHA-256 hash.

Open Command Prompt.

In order to create a hash for a particular file (e.g. hashing_example.pdf), find the location of that file on your computer. Then type the following: *certutil -hashfile "c:\XXXXX\YYYYY.ZZZ" SHA 256*. The placeholder "XXXXX" is the file location path, "YYYYY" the file name, and "ZZZ" the file extension, as shown in the following example:



Upon pressing "Enter", the hash is calculated, and the result is displayed:



For the file used in this example, the SHA-256 hash is as follows: 28b21e2a4a1176eaae16b8943c235892b13-f0ee92f58c1d30a82e2e542ab5da4. It is important to note that hashing is unidirectional: The original file cannot be reconstructed from its hash. The hash alone is meaningless without the file, but if the file is available, the same hash can always be recalculated. For example, anyone with the same document can run the hashing algorithm (such as SHA-256) again and obtain the identical hash, thereby showing that this specific file is the one represented by the hash. Furthermore, the hash is entirely content-dependent:

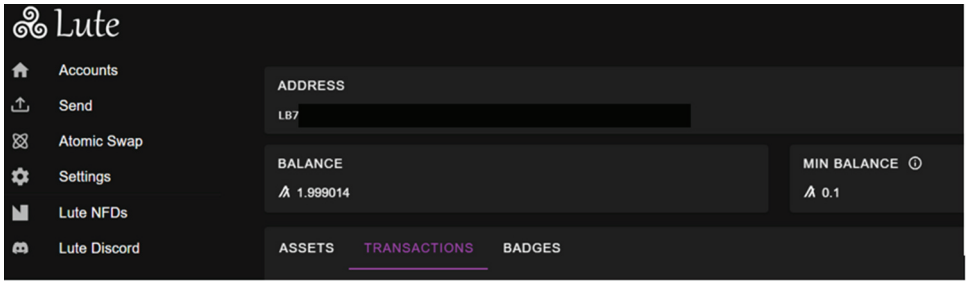
- Changing the file name or storage location does not affect the hash.
- Changing even a single character in the document will produce a completely different hash.
- Saving a file after making a temporary edit (even if the edit is undone before saving) will also alter the hash because the underlying binary representation of the file has changed. Autosaving may change the hash accidentally, and some types of files, such as PDF, may be less vulnerable to unintentional hash changes.

In sum, a hash is a robust digital fingerprint of a document's contents. It ensures that anyone can later verify the integrity of a preregistration or dataset by comparing the stored hash with a freshly generated one.

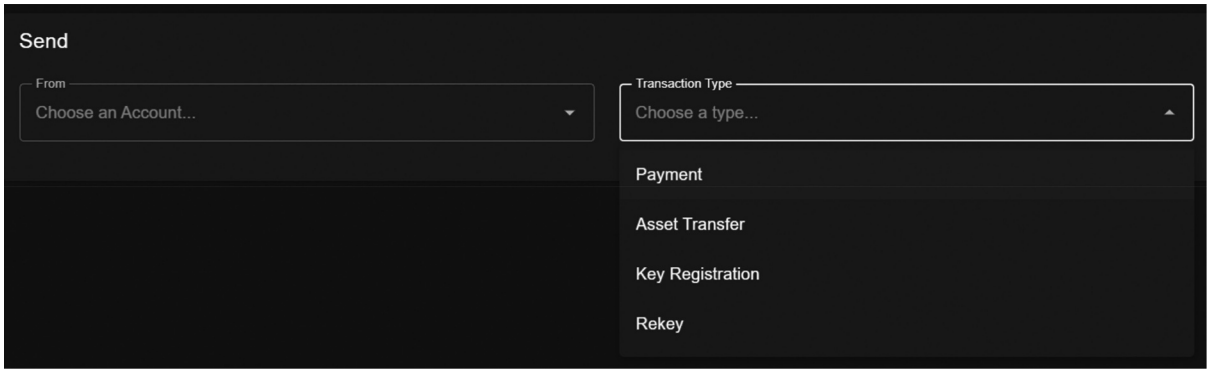
2.2. Step 2: storing the hash on the Algorand blockchain

In this step, the hash will be stored on a blockchain, with an unalterable timestamp. There are several ways to store the information on the blockchain. At the time of writing this article, Lute Wallet (https://lute.app) provides a convenient option. Opening a new wallet requires the user to note down a 25-word code and a wallet address. This wallet allows the user to store the cryptocurrency Algorand. The authors cannot provide any specific advice on how to send Algorand to this address, as this depends on local jurisdiction and personal circumstances. One may use one of the many cryptocurrency exchanges or simply ask a friend to send a small amount of Algorand to this address. Given the very low fees on this network (approximately 0.001 ALGO; with an exchange rate of 1 ALGO = US$0.22 on 23 September 2025), one can create 2000 on-block records of their hash with as little as 2 ALGO.

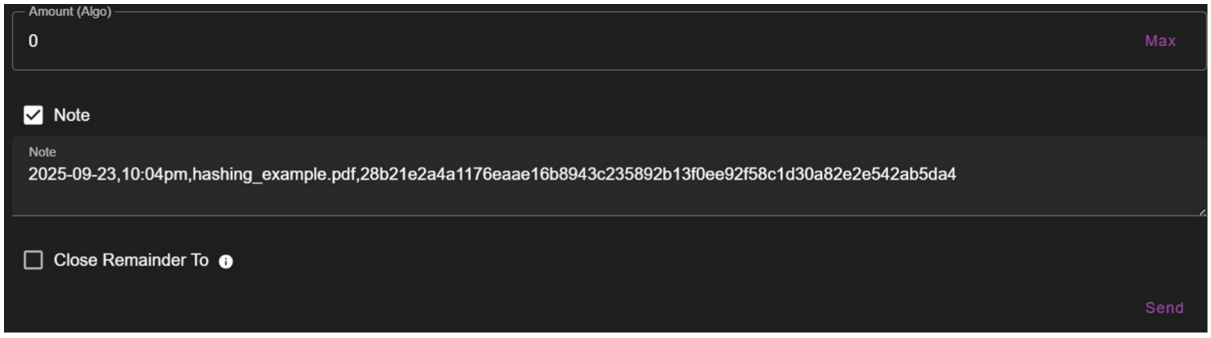
Once a balance appears in the account, one is ready to select "Send":



Here, one needs to select one's account and also select "Payment":



Then select the recipient address as the same address as one's own wallet. The amount to be sent will be 0 ALGO. In other words, an amount of 0 ALGO is sent to the same address. This will only incur the processing fee mentioned earlier. In the field called "Note", one will leave the hash as well as any other information such as a specific transaction code one would like to use. While the blockchain record will automatically store the time of the note creation, one may still prefer to add their own timestamp, such as:



Once the transaction has been confirmed, the user is able to access information about the completed transaction. By clicking on the information, one is then automatically led to another website (https://allo.info) where both the timestamp and the note are displayed:

This note will now remain unerasable and as a permanent record of the hash, together with the corresponding timestamp.

2.3. Step 3: storing the transaction information and making it publicly available

Lastly, it is recommended to save the transaction ID, which is prominently displayed at the top of the record:

With this transaction ID, anybody is later able to find the record on https://allo.info or https://explorer.perawallet.app. The transaction ID and content will also be automatically saved in the user's Algorand wallet.

When publishing an article reporting on the outcomes of a preregistered study, one could thus include a note as follows: "During the preregistration process, we computed an SHA-256 hash of our protocol and recorded this hash on the Algorand mainnet prior to analysis (Transaction ID: XXXXX). This timestamp provides quantum-resistant proof of existence of the protocol file, verifiable at allo.info".

Critically, researchers must understand that the blockchain stores only the hash – the digital fingerprint – not the actual file itself. The original research document (e.g. preregistration protocol, dataset) must be securely preserved by the researcher, as it cannot be reconstructed from the hash. If the original file is lost, the blockchain record becomes unverifiable. Therefore, robust local backup practices and, where appropriate, parallel archiving on established repositories remain essential complements to blockchain timestamping. Public file storage in combination with timestamping then provides a complete audit trail. Because the archived file is linked from the outset to a specific cryptographic hash that is immutably timestamped, its originality is demonstrable. Any subsequent alteration of the stored file would produce a different hash value; if this does not match the original blockchain record, the discrepancy immediately signals modification. Such mismatches are objectively verifiable and would raise legitimate concerns during audit or replication attempts. Storing the file in a public repository also prevents accidental hash changes such as through autosaving or other unintentional changes to the file. However, most importantly, the strength of this system lies not only in post-hoc detection but also in its preventive function: The knowledge that alterations would be transparently detectable reduces incentives to modify original research materials, thereby strengthening research integrity.

Because the cryptographic hash is platform-independent, researchers are not obligated to rely on any particular repository or service provider. A researcher could, in principle, curate their own research files locally or on any storage medium of their choosing, while the blockchain timestamp provides the independently verifiable proof of when those files existed. This decouples verification from platform dependence, ensuring that the integrity of the timestamp does not depend on the continued operation or trustworthiness of any single institution.

3. Conclusion

Using the method outlined above, one is able to create a unique digital fingerprint of a research artefact such as a data or text file and confirm this hash information together with a timestamp on a blockchain that is considered to be quantum-computing resistant. In other words, one is able to prove possession of a particular file at a particular point in time. This evidence is unalterable and thus convincing proof of possession. Of course, one must not alter the timestamped file in even the most trivial way, as even the slightest change in the file will change the hash completely. However, the unique hash still remains the same when different copies of the file are made, when stored in different locations, or when the file is re-named. A further consideration is that the hash could change if changes are made to the file through upgrading its extension to a later software version.

There are several advantages of using this blockchain method of timestamping. Firstly, preregistration on a platform such as the Open Science Framework (https://osf.io) is completely reliant on the data curation practices of the service provider platform. While this platform will contain information about the time that the application had been uploaded, this information can still be altered by a malicious party. Through timestamping on a quantum-resistant blockchain, in contrast, unalterable proof of the file's existence at a particular point in time is available. One is thus able to prove that certain ideas and hypotheses had already been proposed at a particular point in time. The same applies to datasets: A researcher can demonstrate that a particular dataset is still the original – again, through a unique hash and an unalterable timestamp stored on a public blockchain. Because the hash is unidirectional, it can be illustrated that a hash belongs to a file, and one cannot re-create the file based on a hash. The fact that the hash is stored on a public chain is therefore not a security risk.

Using the Algorand blockchain, the cost of creating blockchain notes is minimal. The note in the example above was charged a fee of less than 0.001 ALGO. At a rate of 1 ALGO as US$0.22, one is thus able to post more than 4500 notes for US$1.00.

Beyond its primary utility for researchers, blockchain timestamping also offers value for reviewers, editors, and meta-scientists. When an author provides the original file, its hash, and

the blockchain transaction ID, these stakeholders can independently verify that the file existed in its precise form at the recorded date – for instance, confirming that a study was genuinely preregistered prior to data collection or that a dataset was not modified after a particular point in time. While such verification scenarios may arise infrequently, the method's greater contribution may be preventive: If timestamping becomes a routine expectation, the knowledge that research materials are linked to immutable temporal records raises the threshold for undetected fraud, discouraging post-hoc modifications and thereby strengthening research quality through deterrence as much as detection.

At the same time, some limitations should be acknowledged. Currently, Algorand notes are restricted to a maximum of 1 KB in size. While this is sufficient for storing hashes, it limits the amount of accompanying metadata that can be included. Furthermore, the method requires manual data management: Researchers must securely store the Algorand transaction ID to ensure continued access to their records even though in some cases entries might also be located through other search strategies (e.g. by wallet address or date range). These practical considerations mean that, although blockchain timestamping offers powerful guarantees of integrity and temporal proof, its use still requires careful planning and responsible data stewardship. The present article was intended simply to provide researchers with an accessible introduction to how this approach can be implemented with minimal prior technical knowledge. More advanced features – such as automated timestamping – fall beyond its scope, as these typically require case-specific solutions and the involvement of IT professionals.

It is also important to note that blockchain timestamping verifies the existence and integrity of a file at a given point in time, but it does not verify the authenticity of the file's contents. A researcher who manipulates data prior to timestamping would simply be creating a tamper-proof record of an already manipulated file. The method thus does not provide a safeguard against misconduct that occurs *before* the hash is generated. One promising avenue for addressing this limitation in future work is combining blockchain timestamping with born-open data practices (Rouder, 2016), in which raw data files are automatically and comprehensively archived at the point of creation without human approval or intervention. Integrating quantum-resistant timestamps into such automated pipelines could provide both temporal proof, and content integrity from the moment data are collected, though the development of such integrated systems remains a task for future research. Such integration is not straightforward; however, as born-open data practices must be reconciled with ethical obligations to protect participant confidentiality. Raw data files may contain information that could identify participants – for example, open-ended survey responses or demographic details – requiring an additional deidentification layer before data can be made publicly accessible.

The present Method article will hopefully contribute to increased awareness of the importance of quantum-resistant timestamping, thus eventually leading to routine integration of this approach within existing open-science platforms. The Algorand blockchain was used as an illustrative example on how timestamping can be conducted. Certainly, work is currently underway to upgrade other blockchains to become resistant to quantum-computing threats (Lele et al., 2025), suggesting that alternative blockchains will ultimately be able to fulfil the same function. More broadly, such approaches align closely with the goals of the emerging decentralised science (DeSci) movement, which seeks to restructure scientific infrastructure by reducing reliance on centralised intermediaries and enabling transparent, independently verifiable research workflows (Weidener & Spreckelsen, 2024). In this sense, quantum-resistant timestamping may represent a foundational infrastructural component for future open and decentralised scientific ecosystems in the age of AI and quantum computing.

Acknowledgements

The first and third authors are Editors-in-Chief of this journal. For that reason, the manuscript peer-review process was overseen by an Associate Editor.

The authors thank the reviewers for their constructive feedback.

Disclosure statement

No potential conflict of interest was reported by the authors. Immediately after having submitted the first version of this manuscript, we computed an SHA-256 hash of the submitted file and recorded this hash on the Algorand mainnet (Transaction ID: E3OHAPZVSVZTTTLKJZF2FAUF4E6U6JER2DA2PBMBLY2CMUGU5RHA). This timestamp provides quantum-resistant proof of existence of this file, verifiable at allo.info.

ORCID

Christian U. Krägeloh http://orcid.org/0000-0002-7298-0736
Emerson J. Bartholomew http://orcid.org/0000-0003-0735-0436
Oleg N. Medvedev http://orcid.org/0000-0002-2167-5002

Generative AI

Generative AI (ChatGPT5 and Claude Sonnet 4.5) was used to improve grammar and wording of sentences.

References

Allende, M., López León, D., Cerón, S., Pareja, A., Pacheco, E., Leal, A., Da Silva, M., Pardo, A., Jones, D., Worrall, D. J., Merriman, B., Gilmore, J., Kitchener, N., & Venegas-Andraca, S. E. (2023). Quantum-resistance in blockchain networks. *Scientific Reports*, *13*(1), 5664. https://doi.org/10.1038/s41598-023-32701-6

Baker, M. (2016). Is there a reproducibility crisis? *Nature*, *533*(7604), 452–454. https://doi.org/10.1038/533452a

Banks, G. C., Field, J. G., Oswald, F. L., O'Boyle, E. H., Landis, R. S., Rupp, D. E., & Rogelberg, S. G. (2019). Answers to 18 questions about open science practices. *Journal of Business & Psychology*, *34*(3), 257–270. https://doi.org/10.1007/s10869-018-9547-8

Boetto, E., Golinelli, D., Carullo, G., & Fantini, M. P. (2021). Frauds in scientific research and how to possibly overcome them. *Journal of Medical Ethics*, *47*(12), e19. https://doi.org/10.1136/medethics-2020-106639

Bogdan, P. C. (2025). One decade into the replication crisis, how have psychological results changed? *Advances in Methods and Practices in Psychological Science*, *8*(2), 1–14. https://doi.org/10.1177/25152459251323480

Cohoon, J. (2024a). *READ**THIS*!! Spam as a threat for open science. *New Media and Society*, *27*(9), 5151–5179. https://doi.org/10.1177/14614448241248655

Cohoon, J. (2024b, February 5). *Establish grant supplements for open science infrastructure security*. Federation of American Scientists. https://fas.org/publication/open-sci-infrastructure-secure/

Craig, R., Cox, A., Tourish, D., & Thorpe, A. (2020). Using retracted journal articles in psychology to understand research misconduct in the social sciences: What is to be done? *Research Policy*, *49*(4), 103930. https://doi.org/10.1016/j.respol.2020.103930

Crüwell, S., van Doorn, J., Etz, A., Makel, M. C., Moshontz, H., Niebaum, J. C., Orben, A., Parsons, S., & Schulte-Mecklenbeck, M. (2019). Seven easy steps to open science: An annotated reading list. *Zeitschrift für Psychologie*, *227*(4), 237–248. https://doi.org/10.1027/2151-2604/a000387

Divya, K., & Priyadarsini, P. S. U. (2025). Securing IoMT data with algorand blockchain, XChaCha20-Poly1305 encryption, and decentralized storage alternatives. *Scientific Reports*, *15*, 23476. https://doi.org/10.1038/s41598-025-08527-9

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: An overview. *PeerJ Computer Science*, *9*, e1705. https://doi.org/10.7717/peerj-cs.1705

Doss, C., Mondschein, J., Shu, D., Wolfson, T., Kopecky, D., Fitton-Kane, V. A., Bush, L., & Tucker, C. (2023). Deepfakes and scientific knowledge dissemination. *Scientific Reports*, *13*(1), 13429. https://doi.org/10.1038/s41598-023-39944-3

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, *8*, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985

Galyashina, E. I., & Nikishin, V. D. (2022). The protection of megascience projects from deepfake technologies threats: Information law aspects. *Journal of Physics: Conference Series*, *2210*(1), 012007. https://doi.org/10.1088/1742-6596/2210/1/012007

Gandhi, M. S., Mulay, C., Durai, K., Murali, G., Masood, J. A. I. S., Vijayarajan, V., Gautam, K., Chakravarthy, N. S. K., Kumar, S. S., Agarwal, S., Murali, S., Vijayasherly, V., Asirvatham, D., Brohi, S., Vignesh, C., & Anbuchelian, S.

(2024). Quantum blockchain: Trends, technologies, and future directions. *IET Quantum Communication*, *5*(1), 1–27. https://doi.org/10.1049/qtc2.12119

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice & Experience*, *52*(1), 66–114. https://doi.org/10.1002/spe.3039

Gipp, B., Breitinger, C., Meuschke, N., & Beel, J. (2017). CryptSubmit: Introducing securely timestamped manuscript submission and peer review feedback using the blockchain. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 3795–3803). IEEE. https://doi.org/10.1109/JCDL.2017.7991588

Hales, A. H., Wesselmann, E. D., & Hilgard, J. (2019). Improving psychological science through transparency and openness: An overview. *Perspectives on Behavior Science*, *42*(1), 13–31. https://doi.org/10.1007/s40614-018-00186-8

Hardwicke, T. E., Thibault, R. T., Clarke, B., Moodie, N., Crüwell, S., Schiavone, S. R., Handcock, S. A., Nghiem, K. A., Mody, F., Eerola, T., & Vazire, S. (2024). Prevalence of transparent research practices in psychology: A cross-sectional study of empirical articles published in 2022. *Advances in Methods and Practices in Psychological Science*, *7*(4), 1–13. https://doi.org/10.1177/25152459241283477

Hardwicke, T. E., Thibault, R. T., Kosie, J. E., Wallach, J. D., Kidwell, M. C., & Ioannidis, J. P. A. (2022). Estimating the prevalence of transparency and reproducibility-related research practices in psychology (2014–2017). *Perspectives on Psychological Science*, *17*(1), 239–251. https://doi.org/10.1177/1745691620979806

Hesse, B. W. (2018). Can psychology walk the walk of open science? *The American Psychologist*, *73*(2), 126–137. https://doi.org/10.1037/amp0000197

Ikeda, A., Yonemitsu, F., Yoshimura, N., Sasaki, K., & Yamada, Y. (2023). Open science platforms fighting clandestine abuses of piracy and phishing: The Open Science Framework case. *PsyArxiv*. https://doi.org/10.31234/osf.io/xtuen

Klein, O., Hardwicke, T. E., Aust, F., Breuer, J., Danielsson, H., Mohr, A. H., IJzerman, H., Nilsonne, G., Vanpaemel, W., & Frank, M. C. (2018). A practical guide for transparency in psychological science. *Collabra Psychology*, *4*(1), 20. https://doi.org/10.1525/collabra.158

Kuznetsov, O., Peliukh, O., Poluyanenko, N., Bohucharskyi, S., & Kolovanova, I. (2023). Comparative analysis of cryptographic hash functions in blockchain systems. In *Proceedings of the 2nd International Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2023-II)* (pp. 81–94). CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3288

Lele, A., Agarwal, V., & Tewari, H. (2025). From theory to implementation of quantum-safe ledgers with XRPL as a case study. In *2025 7th International Conference on Blockchain Computing and Applications (BCCA)* (pp. 145–152). IEEE. https://doi.org/10.1109/BCCA66705.2025.11229538

Levelt, W. J. M., Noort, E., & Drenth, P. J. D. (2012). *Flawed science: The fraudulent research practices of social psychologist Diederik Stapel*. Tilburg University. https://www.commissielevelt.nl

Maxwell, S. E., Lau, M. Y., & Howard, G. S. (2015). Is psychology suffering from a replication crisis? What does "failure to replicate" really mean? *The American Psychologist*, *70*(6), 487–498. https://doi.org/10.1037/a0039400

Munafò, M. R., Nosek, B. A., Bishop, D. V. M., Button, K. S., Chambers, C. D., Percie du Sert, N., Simonsohn, U., Wagenmakers, E.-J., Ware, J. J., & Ioannidis, J. P. A. (2017). A manifesto for reproducible science. *Nature Human Behaviour*, *1*(1), 0021. https://doi.org/10.1038/s41562-016-0021

National Academies of Sciences, Engineering, and Medicine. (2017). *Fostering integrity in research*. National Academies Press. https://doi.org/10.17226/21896

Nosek, B. A., Hardwicke, T. E., Moshontz, H., Allard, A., Corker, K. S., Dreber, A., Fidler, F., Hilgard, J., Kline Struhl, M., Nuijten, M. B., Rohrer, J. M., Romero, F., Scheel, A. M., Scherer, L. D., Schönbrodt, F. D., & Vazire, S. (2022). Replicability, robustness, and reproducibility in psychological science. *Annual Review of Psychology*, *73*(1), 719–748. https://doi.org/10.1146/annurev-psych-020821-114157

Open Science Collaboration. (2015). Estimating the reproducibility of psychological science. *Science*, *349*(6251), aac4716. https://doi.org/10.1126/science.aac4716

Palmbach, D., & Breitinger, F. (2020). Artifacts for detecting timestamp manipulation in NTFS on Windows and their reliability. *Forensic Science International: Digital Investigation*, *32*, 300920. https://doi.org/10.1016/j.fsidi.2020.300920

Pfadt, J. M., Bartoš, F., Godmann, H. R., Waaijers, M., Groot, L., Heo, I., Mensink, L., Nak, J., de Ruiter, J. P., Sarafoglou, A., Siepe, B., Arena, G., Akrong, E., Aust, F., van den Bergh, D., Brenner, W., Doekemeijer, R., Donzallaz, M. C.van Doorn, J., & Wagenmakers, E.-J. (2025). A methodological metamorphosis: The rapid rise of Bayesian inference and open science practices in psychology. *PsyArxiv*. https://doi.org/10.31234/osf.io/ck3js_v1

Phogat, R., Manjunath, B. C., Sabbarwal, B., Bhatnagar, A., Reena, D., & Anand, D. (2023). Misconduct in biomedical research: A meta-analysis and systematic review. *Journal of International Society of Preventive & Community Dentistry*, *13*(3), 185–193. https://doi.org/10.4103/jispcd.JISPCD_220_22

Rouder, J. N. (2016). The what, why, and how of born-open data. *Behavior Research Methods*, *48*(3), 1062–1069. https://doi.org/10.3758/s13428-015-0630-z

Schmidt, S. (2009). Shall we really do it again? The powerful concept of replication is neglected in the social sciences. *Review of General Psychology*, *13*(2), 90–100. https://doi.org/10.1037/a0015108

Selvakumar, A. A. L., & Ganandhas, C. S. (2009). The evaluation report of SHA-256 crypt analysis hash function. In *2009 International Conference on Communication Software and Networks* (pp. 586–592). IEEE. https://doi.org/10.1109/ICCSN.2009.50

Stroebe, W., Postmes, T., & Spears, R. (2012). Scientific misconduct and the myth of self-correction in science. *Perspectives on Psychological Science*, *7*(6), 670–688. https://doi.org/10.1177/1745691612460687

Weidener, L., & Spreckelsen, C. (2024). Decentralized science (DeSci): Definition, shared values, and guiding principles. *Frontiers in Blockchain*, *7*, 1375763. https://doi.org/10.3389/fbloc.2024.1375763

Wittek, K., Krakau, D., Wittek, N., Lawton, J., & Pohlmann, N. (2020). Integrating Bloxberg's proof of existence service with MATLAB. *Frontiers in Blockchain*, *3*, 546264. https://doi.org/10.3389/fbloc.2020.546264

Xie, Y., Wang, K., & Kong, Y. (2021). Prevalence of research misconduct and questionable research practices: A systematic review and meta-analysis. *Science and Engineering Ethics*, *27*(4), 41. https://doi.org/10.1007/s11948-021-00314-9

Zhaolu, T., Wan, Z., & Wang, H. (2025). Post-quantum rollup: Falcon signature aggregation based on SNARG with enhanced gates. *IEEE Transactions on Information Forensics and Security*, *20*, 2899–2914. https://doi.org/10.1109/TIFS.2025.3544490