



METHOD ARTICLE

How blockchain-timestamped protocols could improve the trustworthiness of medical science [version 1; referees: 2 approved]

Greg Irving¹, John Holden²

¹Institute of Public Health, University of Cambridge, Cambridge, CB2 0SR, UK

²General Practitioner, Garswood Surgery, St. Helens, Lancashire, WN4 0XD, UK

v1 **First published:** 26 Feb 2016, 5:222 (doi: [10.12688/f1000research.8114.1](https://doi.org/10.12688/f1000research.8114.1))
Second version: 25 May 2016, 5:222 (doi: [10.12688/f1000research.8114.2](https://doi.org/10.12688/f1000research.8114.2))
Latest published: 30 Mar 2017, 5:222 (doi: [10.12688/f1000research.8114.3](https://doi.org/10.12688/f1000research.8114.3))

Abstract

Trust in scientific research is diminished by evidence that data are being manipulated. Outcome switching, data dredging and selective publication are some of the problems that undermine the integrity of published research. Here we report a proof-of-concept study using a 'blockchain' as a low cost, independently verifiable method that could be widely and readily used to audit and confirm the reliability of scientific studies.



This article is included in the [All trials matter](#) collection.

Open Peer Review

Referee Status: ✓ ✓ ✓ ✗

	Invited Referees			
	1	2	3	4
version 3 published 30 Mar 2017				✗ report
version 2 published 25 May 2016			✓ report	
version 1 published 26 Feb 2016	✓ report	✓ report		

- 1 **Amy I Price** , University of Oxford UK
- 2 **Luís Pinho-Costa** , Fânzeres Family Health Unit Portugal
- 3 **Charilaos Lygidakis** , University of Luxembourg Luxembourg
- 4 **William J. Knottenbelt** , Imperial College London UK

Discuss this article

Comments (0)

Corresponding author: Greg Irving (gi226@cam.ac.uk)

Competing interests: No competing interests were disclosed.

How to cite this article: Irving G and Holden J. **How blockchain-timestamped protocols could improve the trustworthiness of medical science [version 1; referees: 2 approved]** *F1000Research* 2016, **5**:222 (doi: [10.12688/f1000research.8114.1](https://doi.org/10.12688/f1000research.8114.1))

Copyright: © 2016 Irving G and Holden J. This is an open access article distributed under the terms of the [Creative Commons Attribution Licence](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. Data associated with the article are available under the terms of the [Creative Commons Zero "No rights reserved" data waiver](#) (CC0 1.0 Public domain dedication).

Grant information: The author(s) declared that no grants were involved in supporting this work.

First published: 26 Feb 2016, **5**:222 (doi: [10.12688/f1000research.8114.1](https://doi.org/10.12688/f1000research.8114.1))

Trust in scientific research is diminished by evidence that data are being manipulated¹. Outcome switching, data dredging and selective publication are some of the problems that undermine the integrity of published research. The declaration of Helsinki states that every clinical trial must be registered in a publicly accessible database before recruitment of the first subject². Yet despite the creation of numerous trial registries problems such as differences between pre-specified and reported outcomes persist³⁻⁵. If readers doubt the trustworthiness of scientific research then it is largely valueless to them and those they influence. Here we propose using a ‘blockchain’ as a low cost, independently verifiable method that could be widely and readily used to audit and confirm the reliability of scientific studies.

A blockchain is a distributed, permanent, timestamped public ledger of transactions. In doing so it provides a method for establishing the existence of a document at a particular time that can be independently verified by any interested party. When someone wishes to add to it, participants in the network – all of whom have copies of the existing blockchain – run algorithms to evaluate and verify the proposed action. Once the majority of ‘nodes’ confirm that a transaction is valid i.e. matches the blockchain history then the new transaction will be approved and added to the chain. Once a block of data is recorded on a blockchain ledger it is extremely difficult to change or remove it as doing so would require changing the record on many thousands computers worldwide. This prevents tampering or future revision of a submitted timestamped record. Such distributive version control has been increasingly used in fields such as software development, engineering and genetics but to date has not been applied to the reporting of clinical studies.

Methods

In this proof-of-concept study we used publically available documentation from a recently reported randomized control trial^{6,7}. A copy of the clinicaltrials.gov study protocol was prepared based on its pre-specified endpoints and planned analyses which was saved as an unformatted text file⁶ (Dataset 1). The document’s SHA256 digest for the text was then calculated by entering text from the trial protocol into an SHA256 calculator (Xorbin©). This was then converted into a bitcoin private key and corresponding public key using a bitcoin wallet. To do this a new account was created in Strongcoin©⁸ and the SHA256 digest used as the account password (private key). From this Strongcoin© automatically generated a corresponding Advanced Encryption Standard 256 bit public key. An arbitrary amount of bitcoin was then sent to a corresponding bitcoin address. To verify the existence of the document a second researcher was sent the originally prepared unformatted document. An SHA256 digest was created as previously described and a corresponding private key and public key generated. The exact replication of the public key (1AHjCz2oEUTH8js4S8vViC8N-Kph4zCACXH) was then used to prove the documents existence in the blockchain using blockchain.info⁹. The protocol document was then edited to reflect any changes to pre-specified outcomes as reported by the COMPare group³. This was used to create a further SHA256 and corresponding public and private keys³.

Dataset 1. Unformatted text file

<http://dx.doi.org/10.5256/f1000research.8114.d114596>

Results

Incorporating a transaction into the blockchain using a public and private key generated from the SHA256 digest of the trial protocol provided a timestamped record that the protocol was at least as old as the transaction generated. The transaction took under five minutes to complete. The process cost was free as the nominal bitcoin transaction could be retrieved. Researchers were able to search for the transaction on the blockchain, confirm the date when the transaction occurred and verify the authenticity of the original protocol by generating identical public and private keys. Any changes made to the original document generated different public and private keys indicating that protocol had been altered. This included assessment of the edited protocol reflecting pre-specified outcomes not reported or non-pre-specified outcomes now reported in the final paper.

Discussion

Fraud or carelessness in scientific methods erodes the confidence in medicine as a whole which is essential to the performance of its function¹. The method described here provides an immutable record of the existence, integrity and ownership of a specific trial protocol. It is a simple and cheap way of allowing a third party to audit and externally validate outcomes and analyses specified *a-priori* with the findings reported *a-posteriori*. The method prevents researchers from changing endpoints or analyses after seeing their study results without reporting such changes. Transaction codes could be recorded in scientific papers, reference databases or trial registries to facilitate external verification. Making changes to pre-specified text in a document or trying to bury a protocol in a trial registry would simply not be possible. Attempts to fraudulently prepare multiple protocols in advance would be technically possible but would require a considerable amount of advanced planning and would leave behind a publically available trail of evidence that could not be destroyed.

The blockchain offers a number of advantages over trial registries or publishing protocols. Firstly, the blockchain would not be confined to the validation of clinical trials. The approach could be used for a whole range of observational and experimental studies where registries do not currently exist. Secondly, the blockchain provides a real-time timestamped record of a protocol. Such precision is important given persistent problems with protocol registration after trial initiation¹⁰. Thirdly, with over 30,000 trials currently published annually and rising, manual outcome verification is simply not possible¹¹.

Conclusion

The method we have described allows anyone to verify the exact wording and existence of a protocol at a given point in time. It has the potential to support automated, extremely robust verification of pre-specified and reported outcomes. This evidence should increase trust and diminish suspicion in reported data and the conclusions that are drawn.

Data availability

F1000Research: Dataset 1. Unformatted text file, [10.5256/f1000research.8114.d114596](https://doi.org/10.5256/f1000research.8114.d114596)¹²

Author contributions

GI conceived the study. GI designed the experiments. GI and JH carried out the research. GI prepared the first draft of the manuscript. All authors were involved in the revision of the draft manuscript and have agreed to the final content.'

Competing interests

No competing interests were disclosed.

Grant information

The author(s) declared that no grants were involved in supporting this work.

References

1. **House of Commons: Science and Technology Committee. Third Report.** 2016.
[Reference Source](#)
2. **WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects.** 2016.
[Reference Source](#)
3. **COMPare - Full results.** 2016.
[Reference Source](#)
4. Slade E, Drysdale H, Goldacre B, *et al.*: **Discrepancies Between Prespecified and Reported Outcomes.** *Ann Intern Med.* 2015.
[PubMed Abstract](#) | [Publisher Full Text](#)
5. Goldacre B: **How to get all trials reported: audit, better data, and individual accountability.** *PLoS Med.* 2015; 12(4): e1001821.
[PubMed Abstract](#) | [Publisher Full Text](#) | [Free Full Text](#)
6. **The Cardiovascular Diabetes & Ethanol (CASCADE) Trial.** Tabular View - ClinicalTrials.gov. 2016.
[Reference Source](#)
7. Gepner Y, Golan R, Harman-Boehm I, *et al.*: **Effects of Initiating Moderate Alcohol Intake on Cardiometabolic Risk in Adults With Type 2 Diabetes: A 2-Year Randomized, Controlled Trial.** *Ann Intern Med.* 2015; 163(8): 569–79.
[PubMed Abstract](#) | [Publisher Full Text](#)
8. **Strongcoin.** 2016.
[Reference Source](#)
9. **Blockchain info.** 2016.
[Reference Source](#)
10. Anand V, Scales DC, Parshuram CS, *et al.*: **Registration and design alterations of clinical trials in critical care: a cross-sectional observational study.** *Intensive Care Med.* 2014; 40(5): 700–22.
[PubMed Abstract](#) | [Publisher Full Text](#)
11. **Medline trend.** 2016.
[Reference Source](#)
12. Irving G, Holden J: **Dataset 1 in: How blockchain-timestamped protocols could improve the trustworthiness of medical science.** *F1000Research.* 2016.
[Data Source](#)

Open Peer Review

Current Referee Status:  

Version 1

Referee Report 11 May 2016

doi:[10.5256/f1000research.8730.r13757](https://doi.org/10.5256/f1000research.8730.r13757)



Luís Pinho-Costa

Fânzeres Family Health Unit, Gondomar, Portugal

This concept paper describes the potential use of blockchain technology in scientific publishing as a way to establish a timestamped record of study protocols.

The paper presents a logical structure and the individual parts form a coherent whole. The language is clear and objective, and the arguments relevant.

The title is elucidative and enticing. The abstract is presented in a synthetic and meaningful way.

The methods are ingenious and relevant to the formulated aims. Sufficient details is provided, allowing for replication of the experiment. Yet, a more clear delineation of the methodological aspects could be useful for readers not accustomed with the technical standards and tools used by the authors.

The conclusions are supported by the findings. Logical implications are drawn by the authors. Timestamped blockchain technology, as proposed by the authors, could revolutionize scientific publishing.

Competing Interests: No competing interests were disclosed.

I have read this submission. I believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.

Referee Report 29 March 2016

doi:[10.5256/f1000research.8730.r12891](https://doi.org/10.5256/f1000research.8730.r12891)



Amy I Price

Department for Continuing Education, University of Oxford , Oxford, UK

The title is informative and appropriate. The abstract is well done and provides considerable detail in an elegant way that focuses on an original innovation for data security.

The research article is a proof of concept study that explains the model and the rationale for why it is needed and how it will be fit for purpose.

Blockchain improves and expands the role for trial registries or publishing protocols. The approach could be used for RCTs and a whole range of observational and experimental studies where registries are needed but do not currently exist. A blockchain provides a real-time time-stamped record of any study protocol.

Security for data and time stamps that are secure and tamper resistant are a welcome addition for clinical trials databases as is one secure shared location for all trials registry entries. This needs to be flexible enough to register change easily and efficiently. The authors supply real data and it is feasible to accomplish this however for professionals with little time to spare the outside interface will need to be simplified and steps minimized to retain users. Somewhat like GOOGLE search on a white page. Only typing a word from one link is required and the search does all the background algorithm loading to accomplish the task. I am sure this will be the next step in the project.

This present research can be replicated by those with sufficient IT skills and it fulfills a significant gap in research. Social media is full of information on security breaches, data fraud and altered protocols, this would be one way to make registering a valid protocol secure and to reduce concerns about trials transparency as research needs to be registered and reported.

The conclusions are justified and balanced.

Competing Interests: No competing interests were disclosed.

I have read this submission. I believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.
