METHOD ARTICLE

REVISED How blockchain-timestamped protocols could improve the trustworthiness of medical science [version 2; referees: 3 approved]

Greg Irving[1], John Holden[2]

[1]Institute of Public Health, University of Cambridge, Cambridge, CB2 OSR, UK
[2]General Practitioner, Garswood Surgery, St. Helens, Lancashire, WN4 0XD, UK

v2 **First published:** 26 Feb 2016, **5**:222 (doi: 10.12688/f1000research.8114.1)
Latest published: 25 May 2016, **5**:222 (doi: 10.12688/f1000research.8114.2)

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. Methods for using blockchain to provide proof of pre-specified endpoints in clinical trial protocols were first reported by Carlisle. We wished to empirically test such an approach using a clinical trial protocol where outcome switching has previously been reported. Here we confirm the use of blockchain as a low cost, independently verifiable method to audit and confirm the reliability of scientific studies.

This article is included in the All trials matter channel.

Open Peer Review

Referee Status: ✔ ✔ ✔

	Invited Referees 1	2	3
REVISED 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

Discuss this article

Comments (0)

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

How to cite this article: Irving G and Holden J. **How blockchain-timestamped protocols could improve the trustworthiness of medical science [version 2; referees: 3 approved]** *F1000Research* 2016, **5**:222 (doi: 10.12688/f1000research.8114.2)

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

Competing interests: No competing interests were disclosed.

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

Editorial note:

Concerns have been raised about the overlap between Version 1 of this article and a previously published blog by Carlisle, who proposed the method 2 years earlier [Carlisle, Benjamin Gregory. "Proof of prespecified endpoints in medical research with the bitcoin blockchain", 25 August 2014], and that the correction (Version 2) published soon after the original was not sufficient to rectify the overlap.

The case has since been discussed in a Committee of Publication Ethics (COPE) Forum, and COPE advised that the correction was sufficient to correct the scientific literature.

The case has been referred to the University of Cambridge for consideration.

REVISED **Amendments from Version 1**

The method we tested here was first proposed by Carlisle in the grey literature. Clear reference to the previously described method (Reference 6) has been added throughout the revised article.

See referee reports

Introduction

Trust in scientific research is diminished by evidence that data are being manipulated[1]. 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 subject[2]. Yet despite the creation of numerous trial registries problems such as differences between pre-specified and reported outcomes persist[3–5]. If readers doubt the trustworthiness of scientific research then it is largely valueless to them and those they influence. Here we confirm the use of 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, tamper proof public ledger of timestamped transactions. It provides a method for establishing the existence of a transaction 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. A method for using blockchain to provide proof of pre-specified endpoints in clinical trial protocols was first suggested by Carlisle in 2014[6]. We wished to empirically test such an approach using a clinical trial protocol where outcome switching has previously been reported.

Methods

In this study we used publically available documentation from a recently reported randomized control trial[7,8]. A copy of the clinicaltrials.gov study protocol was prepared based on it's pre-specified endpoints and planned analyses which was saved as an unformatted text file[7]. Following a method similar to that described by Carlisle the document's SHA256 digest for the text was then calculated by entering text from the trial protocol into an SHA256 calculator (Xorbin©)[6]. 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©[9] and the SHA256 digest used as the account password (private key)[6]. From this Strongcoin© automatically generated a corresponding Advanced Encryption Standard 256 bit public key[6]. 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, public key and bitcoin address generated[6]. The exact replication of the bitcoin address (1AHjCz2oEUTH8js4S8vViC8NKph4zCACXH) was then used to prove the documents existence in the blockchain using blockchain.info©[10]. The protocol document was then edited to reflect any changes to pre-specified outcomes as reported by the COMPare group[3]. This was used to create a further SHA256 digest and corresponding public, private key and bitcoin address[3].

Dataset 1. Unformatted text file

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

Results

Incorporating a transaction from the bitcoin wallet into the blockchain using a private key generated from the SHA256 digest of the trial protocol timestamped a record of the study protocol. 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 an edited protocol reflecting pre-specified outcomes not reported or non-pre-specified outcomes reported in the final paper.

Discussion

Fraud in scientific methods erodes confidence in medicine as a whole which is essential to performing its function[1]. This study demonstrates that the method described by Carlisle provides an immutable record of the existence, integrity and ownership of a specific trial protocol[6]. 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*. It prevents researchers from changing study end-points or analyses after seeing their study results without reporting such changes[6]. Transaction codes could be recorded in scientific papers, reference databases or trial registries to facilitate external verification. As discussed in the CONSORT guidelines, switching of outcomes in trials is sometimes necessary for perfectly legitimate reasons but this should be disclosed in the final report[11]. The use of blockchain timestamped protocols could facilitate trust in the reporting of this process by providing evidence of precisely when protocol changes took place. At the same time, fraudulent attempts to prepare multiple study protocols in advance would be technically possible but would also leave behind a publically available trail of evidence that could not be destroyed[6].

The blockchain offers a number of advantages over the current approaches used 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 initiation[12]. Thirdly, with over 30,000 trials currently published annually and rising, manual outcome verification is simply not possible[13].

Conclusion

Blockchain-timestamped protocols can allow the exact wording and existence of a protocol at a given point in time to be verified. They have the potential to support automated, extremely robust verification of pre-specified with reported outcomes. This evidence should increase trust in medical science by diminishing suspicion in reported data and the conclusions that are drawn.

Data availability

F1000Research: Dataset 1. Unformatted text file, 10.5256/f1000research.8114.d114596[14]

Author contributions

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.* 2016; **164**(5): 374.
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. Carlisle B: [cited 2016 May 19].
Reference Source
7. **The CArdiovasCulAr Diabetes & Ethanol (CASCADE) Trial.** Tabular View - ClinicalTrials.gov. 2016.
Reference Source
8. 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
9. **Strongcoin.** 2016.
Reference Source
10. **Blockchain info.** 2016.
Reference Source
11. **The CONSORT statement.** [cited 21 May 16].
Reference Source
12. 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
13. **Medline trend.** 2016.
Reference Source
14. 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 2

Referee Report 31 May 2016

doi:10.5256/f1000research.9565.r13759

✔ **Charilaos Lygidakis**
Institute for Health and Behaviour, Research Unit INSIDE, University of Luxembourg, Luxembourg City, Luxembourg

The article provides a proof of concept of a way to tackle some fraudulent techniques of manipulation of research data and protocols. According to the authors, it is possible to employ blockchain in clinical trials and other kinds of studies to deliver a time-stamped record of the protocols, preventing retroactive manipulation and offering a simple and affordable way of auditing and external validation. The authors tested such an approach successfully by using a study protocol from clinicaltrials.gov.

The suggested strategy looks very promising and it would be great to see how it can be streamlined and integrated with CTMS and current registries in a simple manner.

The article is well-written and has a logical structure. The abstract summarises the contents meaningfully, the method employed is appropriate and the conclusions are justified.

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.

Competing Interests: CL is a cofounder and company advisor at Lumos Medica Srl, which provides software solutions for clinical trials.

Version 1

Referee Report 11 May 2016

doi: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.

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.

Competing Interests: No competing interests were disclosed.

Referee Report 29 March 2016

doi: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.

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.

Competing Interests: No competing interests were disclosed.