METHOD ARTICLE

REVISED How blockchain-timestamped protocols could improve the trustworthiness of medical science [version 3; referees: 3 approved, 1 not 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

v3 **First published:** 26 Feb 2016, **5**:222 (doi: 10.12688/f1000research.8114.1)
Second version: 25 May 2016, **5**:222 (doi: 10.12688/f1000research.8114.2)
Latest published: 30 Mar 2017, **5**:222 (doi: 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. 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	4
REVISED version 3 published 30 Mar 2017				✗ report
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

4 **William J. Knottenbelt**, Imperial College London UK

Discuss this article

Comments (3)

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 3; referees: 3 approved, 1 not approved]** *F1000Research* 2017, **5**:222 (doi: 10.12688/f1000research.8114.3)

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.

31st March 2017: Due to concerns raised about the methods and scientific validity of this paper, as well as the completeness of the peer review process (see reader comments on this article), advice from an additional independent peer reviewer with expertise in blockchain technology and cryptography is being sought. We will update this note in due course.

REVISED **Amendments from Version 2**

To clarify our approach to verifying the original transaction we have included text to confirm that this was done using the same Strongcoin© account used to generate the original transaction. We have also replaced the .docx copy of the file used to verify the transaction with the original .txt file.

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 of 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 to generate a 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. The corresponding private key, public key and bitcoin address were confirmed using the original Strongcoin© account and blockchain.info©[6]. 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 which differed to that for the pre-specified protocol and would not allow the private key to be unlocked in Strongcoin©[3].

Dataset 1. Unformatted text file

http://dx.doi.org/10.5256/f1000research.8114.d156051

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. Any changes made to the original document generated a different SHA 256 digest 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 endpoints 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.d156051[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.* 2017.
Data Source

Open Peer Review

Current Referee Status: ✔ ✔ ✔ ✘

Version 3

Referee Report 22 May 2017

doi:10.5256/f1000research.12186.r22913

✘ **William J. Knottenbelt**
Department of Computing, Imperial College London, London, UK

The article proposes the use of a blockchain as a timestamping service to assure the integrity of clinical trial protocols. This appears to be a specific application of the more general idea of using the blockchain to provide time-stamped "proof-of-existence" of various kinds of documents. As one of many examples, one may refer to the web service http://proofofexistence.com and associated publicity (e.g. https://www.youtube.com/watch?v=6YHiuZeWyrE, which dates from December 2013) to see that this idea has been around for some time before the publication of the present article.

The core of the methodology is described in the article as follows:

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 to generate a 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.

I struggle to follow some of the steps described here. Creating a SHA256 digest from a file is OK and straightforward (although this should be done using the file and not via copy and paste of the contents). How this is then "converted into a bitcoin private key and corresponding public key using a bitcoin wallet" does not seem to make sense. Firstly, why involve an untrusted third party like Strongcoin (one of the key goals of blockchain technology being to avoid the need for these)? Secondly, how does the Strongcoin account password relate to the private key generated by Strongcoin? Strongcoin does ask for "A password to encrypt your account" but I should imagine this is only used to protect the wallet, and not to determine the private/public key pair. To test that is indeed the case, I created two accounts using Strongcoin using the same account password (which was the SHA256 hash of the provided document file). I then examined the private key of each account. They are (as one might expect) different. So it seems wrong to suggest that the account password is being used to *generate* or somehow determine the private key. Rather the account password *protects* an arbitrary public/private key pair generated by Strongcoin. The public/private key pair do not themselves seem to be related to the SHA256 hash used as the account password. And so the act of sending an arbitrary amount of bitcoin to the bitcoin address determined by the public key does not seem to fulfill the role of notarising the existence of the document in a satisfactory manner. Nor is there anything in the script/metadata associated with the transaction to

link it to the document. Proofofexistence.com for example uses the OP_RETURN field in the script to store the hash of the document in question (see https://proofofexistence.com/about), which does provide the necessary link. I also do not think that changing the account password would affect the public/private key pair in any way, other than changing the encoding used to encrypt them.

In terms of the verification protocol:

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. The corresponding private key, public key and bitcoin address were confirmed using the original Strongcoin© account and blockchain.info©[6].

This is fine as far as creating the SHA256 digest is concerned. Where it seems to go awry is in requiring "the original Strongcoin account" to confirm the corresponding private key, public key and bitcoin address. Other researchers won't have access to this account (and if they do, they can use it to send themselves the Bitcoin that was sent to it in the first place). Further, even if researchers get access to the account (because e.g. the login details are made public), what is there to link the account to the document? Only the password used to encrypt the account (which Strongcoin might already provide a facility to change, or if not, might provide a facility to change in the future).

Perhaps I have misunderstood some aspect of this methodology, but I am happy to go on record as stating that it does not seem to me to be correct.

I am also struggling to see the insight provided by the content of the paper, even if the methodology can be corrected. In my opinion the whole paper could be summarised in two sentences: "Blockchains can provide timestamped proof-of-existence for documents (see e.g. http://proofofexistence.com). So for example you might encode the existence of a clinical trial protocol in a blockchain to ensure it is not subsequently tampered with."; since this is arguably the point of one of the references published some years previously (https://www.bgcarlisle.com/blog/2014/08/25/proof-of-prespecified-endpoints-in-medical-research-with-the , which incidentally contains an alarming similar methodology), I do not see value in publishing the present work. Nor can I see the value in stating something along the lines of "I used a service like http://proofofexistence.com to upload a hash of a document, which happened to be a clinical trial protocol, onto the Bitcoin blockchain, and then I verified that I could check for the hash of the document."

Is the rationale for developing the new method (or application) clearly explained?
Yes

Is the description of the method technically sound?
No

Are sufficient details provided to allow replication of the method development and its use by others?
No

If any results are presented, are all the source data underlying the results available to ensure full reproducibility?
Partly

Are the conclusions about the method and its performance adequately supported by the findings presented in the article?
No

Competing Interests: No competing interests were disclosed.

Referee Expertise: Cryptocurrency and Blockchain Research

I have read this submission. I believe that I have an appropriate level of expertise to state that I do not consider it to be of an acceptable scientific standard, for reasons outlined above.

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.

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

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.

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.

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

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.

Discuss this Article

Version 3

Author Response 01 Apr 2017

Greg Irving, University of Cambridge, UK

We thank Himmelstein for his comments. We have provided the journal with the unformatted text file discussed. The approach used by Himmelstein differed from ours in that we verified the initial transaction by using the Strongcoin©account to generate the original bitcoin transaction. This is clarified in the updated version. We agree that the Strongcoin© password is not the private key and have explained that this is required to unlock the private key. We accept that this approach has limitations in that a Strongcoin© login is required to verify the private key and the associated time-stamped public key. Alternative approaches to generating a private key such as those discussed by Himmelstein could be an improvement upon those we proposed in that it would not rely on access to the original Strongcoin© account.

Competing Interests: None

Reader Comment 30 Mar 2017

Daniel Himmelstein, University of Pennsylvania, USA

In Version 3 of the article, Irving & Holden concede they used the protocol's hash as a wallet password and not a private key. Accordingly, there is no timestamp of the clinical trial protocol in the Bitcoin blockchain. Irving & Holden have failed, and will continue to fail, to provide crypographic proof that the protocol existed on February 11, 2016.

I've added an update to my blog post with further details. Also see this PDF diff of the changes between versions 2 and 3 of this study, contributed by Benjamin Carlisle. In summary, Irving & Holden's implementation is broken. Version 3 of the study now more clearly describes the broken method, but does not address the fact that it's broken.

Competing Interests: No competing interests were disclosed.

Version 2

Reader Comment 09 Mar 2017

Daniel Himmelstein, University of Pennsylvania, USA

I've reviewed version 1 & 2 of this study. As I detail in a blog post, Irving & Holden's address generation appears to be broken. I could not verify the protocol's timestamp and hence deem the study irreproducible. There is no proof of existence in the bitcoin blockchain for the protocol that I could uncover. The source code and data for my analysis are available on GitHub (archive).

I encourage Irving & Holden to consult with the "second researcher" that replicated the address generation and publicly provide the cryptographic chain of operations that verifies their timestamp. Absent this validation, the study is meritless.

Competing Interests: No competing interests were disclosed.