METHOD ARTICLE

REVISED Blockchain protocols in clinical trials: Transparency and traceability of consent [version 3; referees: 1 approved, 1 not approved]

Mehdi Benchoufi [1], Raphael Porcher[1], Philippe Ravaud[1,2]

[1]Département d'Epidémiologie Clinique, APHP, Paris, France
[2]Centre de recherche Inserm Epidémiologie et Statistique Paris Sorbonne Cité (U1153), Université Paris Descartes, Paris, France

v3 **First published:** 23 Jan 2017, **6**:66 (doi: 10.12688/f1000research.10531.1)
Second version: 27 Apr 2017, **6**:66 (doi: 10.12688/f1000research.10531.2)
Latest published: 04 Jul 2017, **6**:66 (doi: 10.12688/f1000research.10531.3)

Abstract

Clinical trial consent for protocols and their revisions should be transparent for patients and traceable for stakeholders. Our goal is to implement a process allowing the collection of patients' informed consent, which is bound to protocol revisions, storing and tracking the consent in a secure, unfalsifiable and publicly verifiable way, and enabling the sharing of this information in real time. For that, we will built a consent workflow using a rising technology called Blockchain. This is a distributed technology that brings a built-in layer of transparency and traceability. From a more general and prospective point of view, we believe Blockchain technology brings a paradigmatical shift to the entire clinical research field. We designed a Proof-of-Concept protocol consisting of time-stamping each step of the patient's consent collection using Blockchain; thus archiving and historicising the consent through cryptographic validation in a securely unfalsifiable and transparent way. For each revision of the protocol, consent was sought again. We obtained a single document, in a standard open format, that accounted for the whole consent collection process: timestamped consent status with regards to each version of the protocol. This document cannot be corrupted, and can be checked on any dedicated public website. It should be considered as a robust proof of data. However, in a live clinical trial, the authentication system should be strengthened in order to remove the need for third parties, here the trial stakeholders, and give participative control to the peer-to-peer users. In the future, we think that the complex data flow of a clinical trial can be tracked using Blockchain, that a blockchain core functionality, named Smart Contract, could help prevent clinical trial events not to happen in the right chronological order: for example including patients before they consented or analysing case report forms data before freezing the database. Globally, we think Blockchain will help with reliability, security, and transparency, and could be a consistent step towards reproducibility.

This article is included in the All trials matter collection.

Open Peer Review

Referee Status: ✔ ✘

	Invited Referees 1	2
REVISED version 3 published 04 Jul 2017		✘ report
REVISED version 2 published 27 Apr 2017		✘ report
version 1 published 23 Jan 2017	✔ report	✘ report

1 **Mike Clarke**, Queen's University Belfast, Ireland

2 **Daniel S. Himmelstein**, University of Pennsylvania, USA

Discuss this article

Comments (1)

Corresponding author: Mehdi Benchoufi (mehdi.benchoufi@aphp.fr)

Author roles: Benchoufi M: Conceptualization, Project Administration, Software, Writing – Original Draft Preparation; **Porcher R**: Conceptualization, Methodology, Supervision, Writing – Review & Editing; **Ravaud P**: Conceptualization, Methodology, Supervision, Writing – Review & Editing

Competing interests: No competing interests were disclosed.

How to cite this article: Benchoufi M, Porcher R and Ravaud P. **Blockchain protocols in clinical trials: Transparency and traceability of consent [version 3; referees: 1 approved, 1 not approved]** *F1000Research* 2017, **6**:66 (doi: 10.12688/f1000research.10531.3)

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

First published: 23 Jan 2017, **6**:66 (doi: 10.12688/f1000research.10531.1)

REVISED **Amendments from Version 2**

Mainly, we resize strictly and focus the global scope of the current article. We define what can be directly implemented in a live clinical trial and we sketch what would be the key elements to build in order to achieve a trustless consent process. This discussion is strongly connected with the issue of distributing the cryptographic key generation process which enables authentication.

Also, we suppress from the introduction section the development related to the community empowerment since it supposes to exploit the distributed nature of the network trust and that the actual state of the implementation, especially the cryptographic keys generation, still relies on a third party. We referred this part to the discussion section. Besides, we state more clearly what belongs to the current implementation of the POC and what belongs to more prospective thoughts. We detailed the informations regarding the step-by-step proof of process related to Chainscript and other issues from a security point of view.

See referee reports

Introduction

Patient participation is the *sine qua non* condition for clinical trials to happen and for medical research to improve[1,2] (http://www.mc.vanderbilt.edu/crc/workshop_files/2011-09-09.pptx). However, in practice, the informed consent process is hard to handle in a rigorous and satisfactory way. The US Food and Drug Administration (FDA) reports some metrics that are related to the frequency of clinical investigator-related deficiencies, which show that almost 10% of trials they monitored suffer from consent collection issues, such as failure to re-consent when new information becomes available, use of expired forms or non-validated, unapproved forms, consent document not signed or not dated, missing pages in consent document provided to participants, failure to obtain written informed consent, parental permission obtained after child assent, changes made to the consent documents by hand and without IRB approval[3,4] (http://www.fda.gov/downloads/AboutFDA/CentersOffices/CDER/UCM256376.pdf; http://www.yale.edu/hrpp/education/documents/CommonProblemsinInformedConsent_2013_vF.pptx). The study by Seife[5] analysed hundreds of clinical trial FDA inspection documents, covering the 1998–2013 period, and showed that a substantial number of them presented evidence of research misconduct, among which 53% were related to failure to protect the safety of patients and/or issues with oversight or informed consent.

This can lead to dramatic events, as in France in January 2016: a trial testing the "BIA 10-2474" as an analgesic molecule caused the death of a participant. The French health agency IGAS appeared to prove that re-consent was not sought after major neurological side effects occurred in some patients, leading to participants being included in the clinical trial without being informed of this issue and still receiving doses of the analgesic molecule, (http://www.liberation.fr/france/2016/02/04/drame-de-l-essai-clinique-a-rennes-le-deces-reste-inexplique_1431074; https://fr.wikipedia.org/wiki/BIA_10-2474, version of 2016.09.05). Another example in the UK occurred when a general practitioner was struck off after testing drugs on patients who did not give their consent[6]. A recent, popular case of serious scientific misconduct was the DECREASE studies performed by Don Poldermans. The results of these studies were invalidated and some related publications retracted as, amongst many other frauds including data invention, informed consent was not proved to have been obtained before the randomised controlled trials (https://en.wikipedia.org/wiki/Don_Poldermans, version of 2016.09.05; http://retractionwatch.com/category/by-author/don-poldermans/).

Obtaining an individual's consent is strictly tied to the Helsinki declaration[7,8] (http://www.wma.net/en/30publications/10policies/b3/index.html), which provides the good practices that should follow any stakeholder conducting a clinical trial. Point 26 of the Declaration states that each participant should be informed of the aim, methods, sources of funding, conflict of interests, affiliations of the researchers, anticipated benefits and risks and post-study provisions, and these conditions must be met to obtain freely-given informed consent. In practice, regulation agencies, such as the FDA, provide recommendations and mandatory commitments for consent to be collected in the right conditions[9] (http://www.fda.gov/downloads/RegulatoryInformation/Guidances/UCM405006.pdf). Among those and of major importance, informed consent should be documented by a signed and dated written consent, which is particularly meaningful with Blockchain technology.

In addition, consent collection is a dynamic process; it is not a one-shot process ending when consent is sought before a clinical trial begins. As explained by Gupta[1], there are circumstances under which consent has to be sought again from a participant, corresponding to any time the trial protocol is majorly revised. This is a fundamental fact when ensuring to patients' rights and transparency of a clinical trial[10,11]. Indeed, as detailed in these Institutional review board (IRB) guidelines (http://www.irb.pitt.edu/sites/default/files/reconsent guidance.pdf; http://www.mayo.edu/research/documents/29-re-consent-or-notification-of-significant-new-findingspdf/doc-10027714; http://www.yale.edu/hrpp/policies/documents/Reconsentingguidance.pdf), there are many situations where patients re-consent has to be sought or where they should be notified of minor trial issues, such as novel risks, significant changes in the research procedures, and worsening of the medical condition. Documents that are to be sent to patients can be consent form addendums, an information letter or a fully revised consent form. Of course, the revised consent form has to be approved by an IRB. It must be stressed that the FDA has highlighted the necessity to conceive a mechanism that ensures that the most recent revised consent form is in use in a clinical trial, and stipulates that timestamping is such an approved mechanism[9] (http://www.fda.gov/downloads/RegulatoryInformation/Guidances/UCM405006.pdf).

As indicated in Figure 1, consent is a dynamic process that involves a complex circuit of data and interacting actors, which should all retain information of this on-going process. For example: what participants were notified; when the notifications were delivered; whom of the participants consented or re-consented; when did participants consent or re-consent. This information should circulate between the clinical trial stakeholders in real time.

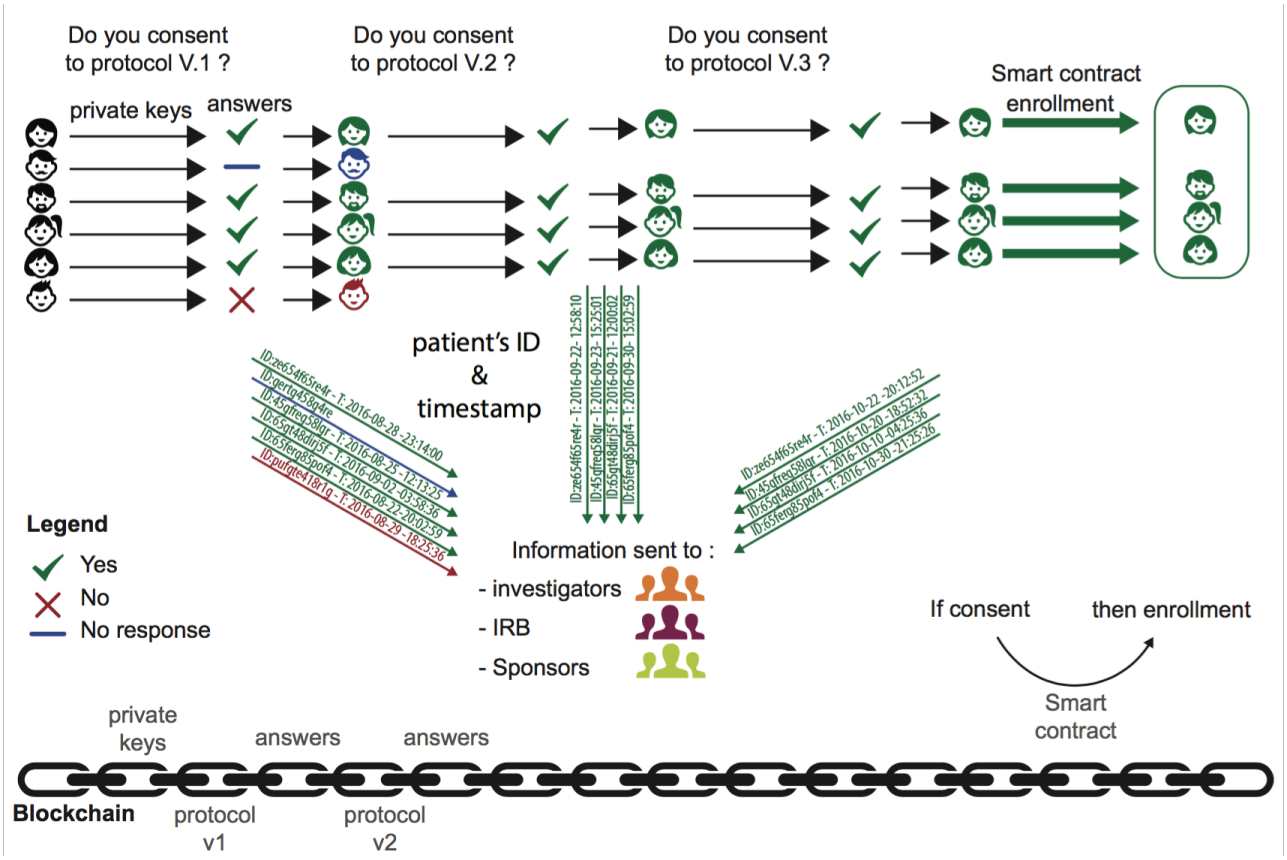

Figure 1. Consent collection Blockchain workflow.

Blockchain is a dawn-aged technology, a giant public datastore, stored in a secure and decentralised way (see Sotoshi Nakamoto seminal paper, https://bitcoin.org/bitcoin.pdf). It is widely announced to be a backbone of the circulation of digital assets, powering any kind of services by transparency, traceability. In this context, Blockchain's emerging and promising technology (https://en.wikipedia.org/wiki/Blockchain_(database)) can bring solid basis in the enrolment phase transparently to all stakeholders of a clinical trial, especially in the context of obtaining participant's consent. Three core functional principles of this technology can play a fundamental role, as follows:

1. Unfalsifiable timestamping information: this stands for proof of existence of any piece of data. When stored, this data is provable and immutable through a strong cryptographic protocol. Moreover, these proofs of existence can be checked on a public website (https://opentimestamps.org, https://arxiv.org/abs/1502.04015). This transparency is of interest to any interested stakeholder.

2. Smart contract: this is a contract that is algorithmically implemented and binds any change in the protocol to the patients' consent seeking renewal.

3. The decentralized nature of the Blockchain protocol gives to the patient, or more widely to patients' communities, control over their consent and its revocation. The end-to-end connectivity creates a network that empowers patients and researchers as peers.

The current implementation is an application of the first principle. Ideally, we would have to build a patient authentication system which does not relies on any trial stackholder, this way we can benefit from the decentralised and trustless nature of the blockchain network.

Let's note in a broader clinical trial setting that it follows directly from the secure timestamping functionality that Blockchain can help prevent from a posteriori reconstruction of endpoints or outcomes in clinical trials, (http://www.bgcarlisle.com/blog/2014/08/25/proof-of-prespecified-endpoints-in-medical-research-with-the-bitcoin-blockchain/).

Blockchain comes into play

At a clinical trial level. Blockchain technology can act as a SafeGuard for the complex and wide range of actors required in clinical trials. In practice, the proof of existence for consent will be timestamped and stored in Blockchains, enabling clinical research stakeholders, such as sponsors, investigators and IRBs, which can be numerous in multi-center clinical investigations, to share consent and re-consent related data in real-time, and archive and historicize consent sets, which can be matched with each revision of the protocol.

At a patient level. Implementing a "privacy by design" technology, and archiving securely and transparently any dataset that needs to be stored, is a game changer towards improving enrolment phase methodology. Moreover, drawing on ways to collect securely and transparently informed consent, being careful with participants rights, and so empowering them, could improve the enrolment rate. Indeed, the participation rate to clinical trial remains quite weak[10]. Caldwell & All performed a systematic review comparing different enrolment techniques, and showed that, amongst several other explanations, the conditions of collecting patients consent in an open and secure way is better at achieving an improved rate of enrolment[10,12].

Methods

In this proof-of-concept (POC) study, we targeted 27 volunteers for enrolment, which was achieved at the Clinical Epidemiology Department at Hospital Hôtel Dieu (Paris, France). There were no exclusion or inclusion criteria; the volunteers that were recruited were staff members of the Epidemiology Department (Hospital Hôtel Dieu). However, we ensured each of the users had email access.

A fake experimental clinical trial protocol was designed whose purpose was to compare the effect of "cisplatin vs. ledgerlin", the last substance being a neologism, which was derived from the critical public datastore shared by all Blockchain users called "ledger". The protocol was accompanied by a consent form, which mimicked a design used routinely.

Each of the to-be-enrolled users were assigned a private key in order to sign data and documents, and in practice this would be used to publish their signed consent, which was to be anchored to the Blockchain.

Blockchain networks

There are several Blockchain networks, for example Ethereum (https://www.ethereum.org), Bitcoin (https://en.wikipedia.org/wiki/Bitcoin_network) and Hyperledger (https://www.hyperledger.org). For our purpose, transactions and their validations were run on the Bitcoin network. Our choice was motivated by stability and immutability of the Bitcoin Blockchain, due to its large mining network, and the API it provides facilitates development. Moreover, it is the more widely used Blockchain network; therefore, there is a relatively dense community of developers to enable an efficient support (https://bitcoin.stackexchange.com). The front-end and back-end technologies that are detailed hereafter were implemented by a Blockchain solutions provider, Stratumn SAS (https://stratumn.com/).

A website was developed with a simple one-page interface (Figure 2). On the front-end, it displayed the consent document, a checkbox attesting that the protocol was read and understood, and a push button that triggered the consent process.

In practice, the on-line signed document contained a piece of code called "Chainscript", (http://chainscript.io), which contained all the critical information about the user, and the version of the protocol attached to the signature. Each proof of signature had a manifest that takes the form of a hash that is the digital proof of signature.

On the back-end, pressing the "consent button" triggers Blockchain transactions: the proof of signature is timestamped and stored in the Blockchain. It should be emphasised that these signatures were shared in real-time through a restricted group of individuals, namely the present authors, who stand, in a real-life implementation, for investigators, IRBs or sponsors. This group obtains access to a dashboard (Figure 3) with the following: an admin panel displaying the consent status of each user; the protocol that transparently stores the public keys of each consenting user (through Chainscript); and the history of each released version of the protocol and the consent and re-consent of the user attached to each of these versions.

Authentication method

For each user a pair of private-public keys were provided, (https://msdn.microsoft.com/fr-fr/library/windows/desktop/aa387460(v=vs.85).aspx). These are asymmetric cryptographic data that enables authentication on Blockchain. These were randomly attached in one-to-one correspondence to a user's emails. We focused our interest to Blockchain's usage in the time-stamping and archiving logic. We did not let users create or use their own Blockchain authentication setup, i.e. if a user owned a Bitcoin account, the key and Bitcoin address were not allowed to be used. This restriction was not related to Blockchain complexity, but rather to maintain a simple and common email-focused authentication process. Other ways exist for authentication, such as physical devices, like USB keys or cell phone fingerprints, but this would have led us far from the focus point of our protocol-related problematics.

Workflow

The process that participants were submitted is as follows:

- The study investigators to send email to the patients.
- The users receive the email, which contains a web hyperlink redirecting them to the web interface that displays the consent form.
- In the background, after clicking the consent button without the user experience being bothered by any blockchain transaction related complexity, the user signature is registered to the Blockchain and is timestamped.
- Each time the protocol is updated, investigators send an email explaining the major changes that occurred and users are invited to sign the revised consent form.
- Each step of this process is updated on the investigators' admin panel with the version of the consent document and the user's consenting status.

Proof of existence - Chainscript

Signatures of the evolving consent document were registered to the Blockchain. Moreover, all of the relevant interactions of the user with our platform was stored in the Blockchain, i.e. the consent form upload by the investigator; email requests to users; and patient

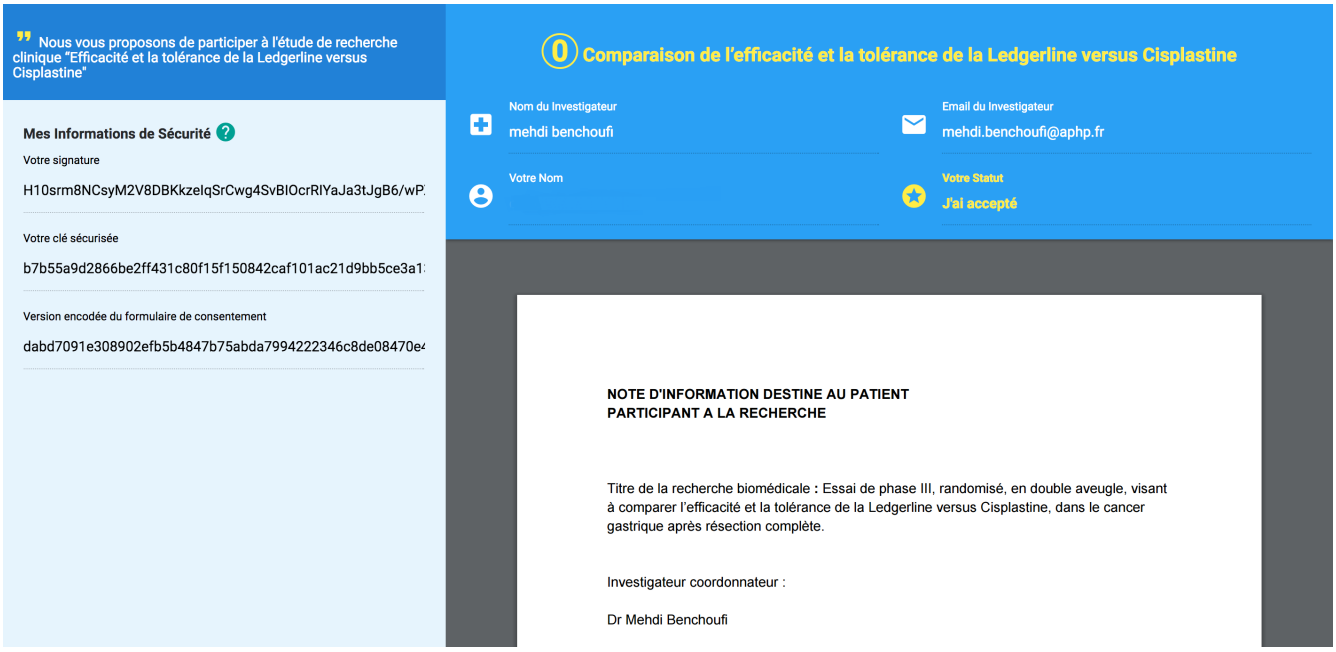

Figure 2. Patients web-interface for blockchained consent collection website.

Figure 3. Investigator dashboard for blockchained consent collection website.

signatures. This is done accordingly to the Proof-of-Process concept developed by Stratumn, which is a method for proving the integrity of a process between partners (https://stratumn.com/pdf/proof-of-process.pdf).

The piece of data attesting and synthesising all this information is called a Chainscript. It is a JSON formatted data structure holding all the information related to the protocol and users' consent. Chainscript is a JSON format developed by Stratumn SAS, especially dedicated to attest the steps in trusted workflows (http://chainscript.io/). Chainscript is an open standard. The philosophy behind it is to be able to prove the integrity of a process with a single JSON data structure by securing the who, when, what and where of a sequences of steps that are linked together in chronological order. Each sequence corresponds to a segment, and each segment holds some metadata, an identifier called a hash, and a pointer to the preceding segment. The critical information maintained in Chainscript are the hashes, which are the proofs of the existence of data. Since each Blockchain transaction has a cost, we decided to group the transactions. What makes Chainscript interesting is that a series of Blockchain transactions can be wrapped into the same logic flow, preventing too intensive requesting to the Blockchain network, which can prove to be costly.

Therefore, with this information, how can we check proof of a specific data after they are merged? The ChainScript solution relies on a singular data structure, a Merkle Tree, which in a way "hashes the hash", preserving in one single hash all the hashes, so that if any hash is corrupted, the entire tree is invalidated.

In our implementation, the ChainScript code is held in the PDF consent document, storing its hashed content, all its versions (corresponding to protocol revisions) and all the signing users for each version. It is of major interest that ChainScript can be publicly verified without any proprietary tool.

We should remark that a positive side effect of tracking each step of a user's interaction with the platform is that storing so exhaustively the data, raises the barrier to fraud.

Results

Clinical trial master document

We were able to collect consent and re-consent of users and store them in a transparent, unfalsifiable, verifiable way. These data were encoded in a single document. This document holds the stakeholders' identifiers, the users' identifiers, timestamps of the protocols being sent, consent status, timestamps of the consent, and the version of the protocol to which the consent is attached.

This master document was shared in real-time through key actors that ruled the POC study. It was registered to the Blockchain in a safe way, so that this group of stakeholders retains the timestamped proof of the consent status in an immutable document. We stress again the fact that this document is incorruptible, and it is possible to check its consistency on any dedicated public website (e.g. a website that enables checking of Bitcoin transactions), proving the correspondence between each version of the protocol and its related consent.

Technically, these data are synthesized in the open data format we mentioned earlier, Chainscript, which is as follows:

```
"segment": {
  "link": {
    "state": {
      fileName: "protocole.pdf";
      uploadedBy: "investigateur";
    },
    "meta": {
      "title" : "Protocole",
      "tags" : ["POC", "Essai clinique",
"Hôpital Hôtel-Dieu"],
      "priority": "0"
      "updatedAt": 1455532426303,
      "mapId": "56c11d0ea55773bc6e681fde",
    }
  },
 [{ "Document_ID": "NOTE D INFORMATION
DESTINEE AU PATIENT.pdf"",
  "Doctor_Name": "***",
  "Doctor_Email": "***@aphp.fr",
  "PDF_Title": "",
  "Conditions": "",
  "ExpiresIn": "XX",
  "Max_Patients": "XXX",
  Invites:
  [{
  "Email": "***@aphp.fr",
  "Name": "***",
  "Address": {
     "hash": "2568ce846c1391d94065df6cc4a42720369bcec9",
     "type": "pubkeyhash",
     "network": "livenet"
     }
  },],
  },[
        "signature",
    "***",
    "***@aphp.fr",
    0,
    "H6qy9U3S+BNqreKwMgEnDAHij3wNMcq4T2+
       X9axzx65Zd+HDy16tr03YPT4oKkGtW820so0D+
       0Pk2UTrwnXiLKs=",
    {
         hash:
"6786ce716b2ac8e14b20e0a2fd8b88a7994d4a10",
         type: "pubkeyhash",
         network: "livenet"
    },
         "2016-07-08T13:11:15.824Z",
         "method__saveSignature"
],[{
         "DateSigned": "2016-07-08T13:11:15.824Z",
```

```
"Signature":
 "H6qy9U3S+BNqreKwMgEnDAHij3wNMcq4T2+X9
 axzx65Zd+HDy16tr03YPT4oKkGtW820so0D+0Pk2
 UTrwnXiLKs=",
Consent: 0
}]
```

All this information is bound together in one data structure, so that the whole set of obtained consent, with their uniquely attached version of the protocol, form an immutable global data. The change of a single element breaks the entire data structure.

In the interest of user confidentiality, the master document cannot be made available.

Technical details of the POC

We sent two versions of the protocol (Supplementary File 1 and Supplementary File 2) during the study, through which we sought the users consent; each consent was attached to a specific version of the protocol.

Users were given a digital signature and secured key, each of which consisted of a hash. Amongst the users of this experimental study, 14 gave their consent to the two versions of the protocol, 9 gave their consent to only one version of the protocol and 2 didn't give their consents at all and 2 did not respond to any consent form.

The interaction of the user with the online interface, namely accepting or refusing to give consent, led to a transaction validated in Blockchain. Each version of the protocol had a unique identifier, called a hash. The hash is uniquely attached to the content of the protocol document. The correspondence between the consent document and the hash is one-to-one, namely if one single letter is changed then the hash is broken.

Figure 4 shows where the identifier of the protocol document is highlighted in the Chainscript master document. Figure 5 displays the investigator identifiers, and Figure 6 reveals the consent status bound to the protocol revision version.

Discussion

Blockchain is an emerging, fast-evolving technology. The boiling atmosphere around development and use of Blockchain is similar to tech development during the early stages of the web: It took several years before formatting as html or css became web standards. Blockchain technologies are gaining more and more attention, and Blockchain networks are proliferating, for example Ethereum, Bitcoin, Hyperledger or private Blockchain networks. It is not clear which of these will impose itself as a blockchain network standard, or even if there will be unique standard one. Public networks are interesting due to the idea of a community driven approach and scalability, but private ones can offer a certain level of customization.

Alongside this fast-developing tech, there are still some infrastructure obstructions that are not yet circumvented, namely delays in transaction validation. On the Bitcoin network, the validation process (via the so-called mining) takes around 10 minutes (https://www.quandl.com/data/BCHAIN/ATRCT-Bitcoin-Average-Transaction-Confirmation-Time). In the present study's context, we

Figure 4. Consent collection master document: unique identifier protocol.

```
- link: {
    - meta: {
        - tags: [
              "1467978354664-NOTE D INFORMATION DESTINEE AU PATIENT.pdf",
              "consent",
              "2c28615f6ad24dbe1f8181bd4a11d2d6f66a0dd8ad155653ee855a62b1f28ca7",
              "method__sendEmail"
          ],
          mapId: "577f92726e27683c12a0aea9",
          agentHash: "3263ac4e62279e355143916a5f03bd06bd3289400add67d4960154c85afb2e97",
          stateHash: "39a830ea6aae7997b3fa9cbabad1c33eebec59a0fbbce4cf74d7e6f23a3b0248",
          prevLinkHash: "649cc059079b0284d4fb6f7eb47aab14292fb123e7b00df6e3e0ef1c2a124e4c",
          action: "sendEmail",
        - arguments: [
            - {
                Document_ID: "1467978354664-NOTE D INFORMATION DESTINEE AU PATIENT.pdf",
                Doctor_Name: [redacted]
                Doctor_Email: [redacted]
                PDF_Title: "Comparaison de l'efficacité et la tolérance de la Ledgerline versus
                Cisplastine",
                Conditions: "Nous vous proposons de participer à l'étude de recherche clinique Efficacité
                et la tolérance de la Ledgerline versus Cisplastine".",
                ExpiresIn: "15",
                Max_Patients: "49",
```



```
- link: {
    - meta: {
        - tags: [
              "1467978354664-NOTE D INFORMATION DESTINEE AU PATIENT.pdf",
              "consent",
              "2c28615f6ad24dbe1f8181bd4a11d2d6f66a0dd8ad155653ee855a62b1f28ca7",
              "method__sendEmail"
          ],
          mapId: "577f92726e27683c12a0aea9",
          agentHash: "3263ac4e62279e355143916a5f03bd06bd3289400add67d4960154c85afb2e97",
          stateHash: "39a830ea6aae7997b3fa9cbabad1c33eebec59a0fbbce4cf74d7e6f23a3b0248",
          prevLinkHash: "649cc059079b0284d4fb6f7eb47aab14292fb123e7b00df6e3e0ef1c2a124e4c",
          action: "sendEmail",
        - arguments: [
            - {
                Document_ID: "1467978354664-NOTE D INFORMATION DESTINEE AU PATIENT.pdf",
                Doctor_Name: "Mehdi Benchoufi",
                Doctor_Email: "benchoufi.mehdi@gmail.com",
                PDF_Title: "Comparaison de l'efficacité et la tolérance de la Ledgerline versus
                Cisplastine",
                Conditions: "Nous vous proposons de participer à l'étude de recherche clinique Efficacité
                et la tolérance de la Ledgerline versus Cisplastine".",
                ExpiresIn: "15",
                Max_Patients: "49",
```


Figure 5. Consent collection master document: investigator identifiers.

are not tied by real-time requirements measured in seconds, and so it is not a major obstruction. Moreover, the ChainScript logic we implemented in our POC allows grouped network request validation, which preserves the Blockchain network from computation overload, and allows to scale our method to a large patient cohort. More generally, to tackle this challenge of scaling the network, in case there is a massive amount of transactions, there are some implementations of Bitcoin-based protocol isolated from the Blockchain, the most renown is called SideChain (https://www.deepdotweb.com/2014/06/26/sidechains-blockchain-2-0/; https://www.reddit.com/r/Bitcoin/comments/2kdxy8/).

Moreover, with regard to the authentication process, we can expect that, when the use of Blockchain's technologies will be more common, there is an important chance that users already possess a Blockchain public-private-key identity. Therefore, sending keys for access and identification later in the signing process will be obsolete. This will require maintenance of a double key attribution (as explained above in the "Authentication method" section) for users that do not have any Blockchain network identity and to be able to take into account those who have already one. In the latter case, verification of the digital signature of these users will have to occur.

One step further, we can schematically consider there are two main issues regarding the consent process, the first one being related to the quality of the process itself and the second one related to the identity of the individual consenting, we chose to focus on the first

Figure 6. Consent collection master document: consents status bound to protocol revision versions.

point, and tackle the issues raised by the FDA[3,4] (https://www.fda.gov/downloads/AboutFDA/CentersOffices/CDER/UCM256376.pdf). Indeed, in this POC study, we aimed to consider problems where existing patients were included in a study in the presence of their physician or staff, so that ensuring that the consenting participant was precisely the one expected to be was not a critical matter. Moreover, in the setting of a real online consent process, there is no chance that a patient who would not effectively consent—for instance if there were some fraudulous operation registering him/her as a consenting participant—would actually participate to the study.

However, the issue related to assert the identity will be of importance in the context of a real clinical trial and should be done in a more secure manner than linking between a participant and his/her digital identity through email address. In a production application, we could implement several solution to secure the digital identity of participants: at least implementing a KYC-like solution to bind digital identities and physical entities — Know Your Customer (KYC) are technics used by fiscal administration or banks to secure their online services. A more advanced technique could use a blockchain-based solution to provide material objects, such as USB keys, holding the cryptographic signatures, which can be unlocked by an easy-to-remember code.

In a context where patients master the key generation process, and applying the same process we detail in this POC, we think that we would be close to attain a trustless consent process, which will promote patients community as a decisive actor of clinical trials. Much literature documents barriers to enrolment, especially when barriers are strongly related to community or ethnicity-related issues[13,14]. We think that the decentralised, transparent and secure nature of Blockchain protocol may meet the conditions for an improved engagement of patient communities in clinical trials. This could help optimize patients enrolment, and in turn, through a more transparent and trusted process, can create a bridge between clinical research teams and patient communities, who are novel incomers in our digital age and whose commitment is critically dependent on building clinical trials as a highly trusted process.

It should be noted that we did not implement a consent revocation workflow. However, there is no issue in transposing at that end the Blockchain transaction logic we implemented for the consent. On that point, we should be careful about the fact that if the consent or its revocation can be given or withdrawn with no problem, these actions cannot be erased from the Blockchain. Indeed, if participants revoked their consent by accident, then the action can be reversed, but data will remain containing the revocation of the consent and the cancellation of this revocation.

In the range of more prospective considerations, we think that obtaining consent must be a 'lock' before participant inclusion in clinical trials, so that investigators won't be able to include a patient in the trial until their consent is collected. To ensure a strict parity between enrolled patients and included patients, we could use a tool coming along with blockchain technologies called the Smart Contract (https://en.wikipedia.org/wiki/Smart_contract, version of 2017.05.26). This is a piece of code that holds a programmatically written contract between as many parties as needed, without any third-party, which executes algorithmically according to the terms provided by the contracting parties. In our context, it would be possible to build a Smart Contract that will be executed with the only condition that patients will only be included when the enrolment is complete. Technically, every Blockchain transactions can have a lock associated to them and transactions can be pending and triggered at an agreed upon contract time. For example, the signature of the consent would trigger the execution of a Smart Contract, that would unlock the edition of an eCRF document.

Finally, we evoked a possible improvement in the enrolment rate, by empowering patients and granting them information and control over the enrolment phase. However, Blockchain is certainly not a "one size fits all" solution to the problem of a low enrolment rate. Indeed, there are many other parameters that interfere with the enrolment, which fall beyond the scope of transparency, user control and reliability that Blockchain technology helps to achieve: age, sex, cultural background, socio-economic factors, lack of educational materials[15], readability and length of consent[16–18], limited awareness about clinical research[19] or patient-physician relationship[20] and momentum of consent request[21]. Besides, the scope of our method did not address the question of consent collected in singular situations, such as intensive care, unconscious patients or psychiatric pathologies.

Conclusion

Keeping track of consent collection is consolidated through the use of Blockchain technology. We have seen in this proof-of-concept study that all consent-related data can leave an unfalsifiable and verifiable fingerprint on the Blockchain. This is important both on the stakeholder's side, letting them prove the existence and the consistency of the data, and on the patient's side, giving them more visibility, transparency, and hence control over their consent.

Moreover, though it was not be the focus of this paper, we anticipate that Blockchain technology, in that it does not rely trust on third party but inversely empowers peer-to-peer users by granting them control over consent agreement and revocation, can help gathering conditions of an improved privacy-respected freely-given consent. Besides, given its decentralized protocol, it can help introduce communities to contemporary clinical research, opening, for clinical reasearch, the path to implementing community management techniques in order to enrol patients using a more targeted approach.

From a global perspective, the application of Blockchain technologies in the context of clinical research is broad and promising. Indeed, tracking the complex data flow with numerous diverse stakeholders, and documenting it in real-time through a timestamping workflow, is a key step towards proving data consistency and inviolability, and will hence improve clinical trial methodology.

Software availability

Latest source code available at: https://github.com/benchoufi/DocChain

Archived source code as at time of publication: doi, 10.5281/zenodo.237040 (https://zenodo.org/record/237040#.WHSxorYrI_V)

Author contributions

Mehdi Benchoufi designed the work, initiated and led the analysis on blockchain impacts in the context of clinical trials. With the co-authors, he contributed to identify consent collection process as a substantial use-case for a blockchain implementation, in the idea of clinical trial transparency and traceability. He designed the blockchain collection website and was the medical coordinator of technical developments. Raphaël Porcher contributed to the design of the work, especially on identifying with the corresponding author which of the consent process steps could be wrapped into a Blockchain process. He has put in perspective the potential of implementing Blockchain in consent process, with regards to information of patients, ethics, data privacy. Philippe Ravaud brought his expertise to consolidate the design of work, identified with the corresponding author the issues related to consent process that should be tracked through Blockchain transactions, especially the ones related to protocol revisions and lack of consent collection renewal. He analysed the results with Raphaël Porcher and the corresponding author and inferred from them improved methodology perspectives that Blokchain draw for the entire field of clinical research. Both Raphaël Porcher and Philippe Ravaud reviewed the article, finally approved the article and agree to be accountable on any part of the article relatively of its accuracy and its integrity.

Competing interests

No competing interests were disclosed.

Grant information

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

Supplementary material

Supplementary File 1: Protocol and consent form (versions 0 and 1) used in the proof-of-concept study (in zipped file) (in French).
Click here to access the data.

Supplementary File 2: Protocol and consent form (versions 0 and 1) used in the proof-of-concept study (in zipped file) (in English).
Click here to access the data.

References

1. Gupta UC: **Informed consent in clinical research: Revisiting few concepts and areas.** *Perspect Clin Res.* 2013; **4**(1): 26–32.
PubMed Abstract | Publisher Full Text | Free Full Text
2. Wendy Lloyd, BA, LPN, CIP,CCRP, Regulatory Affairs and Compliance Specialist: **Part 2 of 3 Part Series: Informed Consent, the process.**
Reference Source
3. **Office of Scientific Investigations, Metrics.** US Food and Drug Administration. 2014.
Reference Source
4. Barney JR, Antisdel M: **Common problems in informed consent.** Human Research Protection Program (HRPP). 2013.
Reference Source
5. Seife C: **Research misconduct identified by the US Food and Drug Administration: out of sight, out of mind, out of the peer-reviewed literature.** *JAMA Intern Med.* 2015; **175**(4): 567–77.
PubMed Abstract | Publisher Full Text
6. Dillner L: **BSE linked to new variant of CJD in humans.** *BMJ.* 1996; **312**(7034): 795–800.
PubMed Abstract | Publisher Full Text | Free Full Text
7. **WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects.**
Reference Source
8. Myles PS, Williamson E, Oakley J, *et al.*: **Ethical and scientific considerations for patient enrollment into concurrent clinical trials.** *Trials.* 2014; **15**: 470.
PubMed Abstract | Publisher Full Text | Free Full Text
9. **Informed Consent Information Sheet Guidance for IRBs, Clinical Investigators, and Sponsors.**
Reference Source
10. Resnik DB: **Re-consenting human subjects: Ethical, legal and practical issues.** *J Med Ethics.* 2009; **35**(11): 656–657.
PubMed Abstract | Publisher Full Text | Free Full Text
11. McDonald AM, Knight RC, Campbell MK, *et al.*: **What influences recruitment to randomised controlled trials? A review of trials funded by two UK funding agencies.** *Trials.* 2006; **7**: 9.
PubMed Abstract | Publisher Full Text | Free Full Text
12. Swanson GM, Ward AJ: **Recruiting minorities into clinical trials: toward a participant-friendly system.** *J Natl Cancer Inst.* 1995; **87**(23): 1747–59.
PubMed Abstract | Publisher Full Text
13. Lovato LC, Hill K, Hertert S, *et al.*: **Recruitment for controlled clinical trials: literature summary and annotated bibliography.** *Control Clin Trials.* 1997; **18**(4): 328–52.
PubMed Abstract | Publisher Full Text
14. Hazen RA, Eder M, Drotar D, *et al.*: **A feasibility trial of a video intervention to improve informed consent for parents of children with leukemia.** *Pediatr Blood Cancer.* 2010; **55**(1): 113–8.
PubMed Abstract | Publisher Full Text | Free Full Text
15. Brehaut JC, Carroll K, Elwyn G, *et al.*: **Informed consent documents do not encourage good-quality decision making.** *J Clin Epidemiol.* 2012; **65**(7): 708–724.
PubMed Abstract | Publisher Full Text
16. Pandiya A: **Readability and comprehensibility of informed consent forms for clinical trials.** *Perspect Clin Res.* 2010; **1**(3): 98–100.
PubMed Abstract | Free Full Text
17. Paris A, Brandt C, Cornu C, *et al.*: **Informed consent document improvement does not increase patients' comprehension in biomedical research.** *Br J Clin Pharmacol.* 2010; **69**(3): 231–237.
PubMed Abstract | Publisher Full Text | Free Full Text
18. Mills EJ, Seely D, Rachlis B, *et al.*: **Barriers to participation in clinical trials of cancer: a meta-analysis and systematic review of patient-reported factors.** *Lancet Oncol.* 2006; **7**(2): 141–148.
PubMed Abstract | Publisher Full Text
19. Caldwell PH, Hamilton S, Tan A, *et al.*: **Strategies for increasing recruitment to randomised controlled trials: systematic review.** *PLoS Med.* 2010; **7**(11): e1000368.
PubMed Abstract | Publisher Full Text | Free Full Text
20. Eder ML, Yamokoski AD, Wittmann PW, *et al.*: **Improving informed consent: suggestions from parents of children with leukemia.** *Pediatrics.* 2007; **119**(4): e849–59.
PubMed Abstract | Publisher Full Text
21. Smyth RM, Jacoby A, Elbourne D: **Deciding to join a perinatal randomised controlled trial: experiences and views of pregnant women enroled in the Magpie Trial.** *Midwifery.* 2012; **28**(4): E478–85.
PubMed Abstract | Publisher Full Text

Open Peer Review

Current Referee Status: ✔ ✘

Version 3

Referee Report 31 July 2017

doi:10.5256/f1000research.12989.r24031

✘ **Daniel S. Himmelstein**
Systems Pharmacology and Translational Therapeutics, Perelman School of Medicine, University of Pennsylvania, Philadelphia, PA, USA

After the previous two rounds of revision, there are still major outstanding issues. The revisions only minimally react to my previous reviews and do not include the substantial changes that would be necessary for me to approve this study. For context, see the changes from version 2 to 3 here.

Here are the main factors weighing on my decision:

1. The digital signature scheme that was implemented is worthless in terms of proving that a participant consented. Hence, I entirely ignore and discount this aspect of the proposal.

2. The "proof of concept" justification provided by the authors for the methodological shortcomings and incomplete nature of their study is frustrating. The authors make statements such as (manuscript typos bolded):

   > The current implementation is an application of the **frst** principle. Ideally, we would have to build a patient authentication system which **does not relies** on any trial **stackholder**

   > It would be possible to build a Smart Contract that will be executed with the only condition that patients will only be included when the **enrolment** is complete.

   The assertion that solutions to these problems will come later is insufficient. The authors have to implement the solutions or cease promoting their benefits. In my opinion, these are unsolved problems. Implementing such solutions is difficult: suggesting that a solution exists but not offering an implementation is therefore worthless.

3. The study continues to overstate its reliance on blockchain technology. As our previous dialogue has confirmed, the study only uses the a blockchain for timestamping. Timestamping is an important addition, but does not justify titling the study "blockchain protocols in clinical trials" nor the abundant discussion of blockchains when their role is relatively minor in the actual proposal.

To help explain my decision, I'll elaborate on the theoretically sound aspects of the authors' proposal. The following workflow is theoretically sound, albeit poorly communicated in the manuscript:

1. A webapp is created to administer an electronic consenting process. The webapp can be designed to enforce a rigid workflow that ensures the right steps are performed in the right order.

2. The user interactions and inputs from the electronic consent process can be recorded via a Chainscript JSON file. Therefore, one can store the digital equivalent of paper forms from a traditional physical consent process.
3. The Chainscript JSON file can be timestamped using the Bitcoin blockchain. This prevents predating the existence of a consent record.

Now while a clear, compelling, and clean implementation of the previous steps would be of interest, the study fails to achieve this. Specifically, the webapp is not publicly hosted, so users can experiment with and observe the proposed electronic consent implementation.

Second, the authors do not provide any Chainscript JSON files for their study. In their previous response to my review, they link to a Chainscript file unrelated to their study. Even more troubling is that their Chainscript example from the manuscript appears to be manually edited from an example Chainscript document rather than computer-generated output from their consent application. As I mentioned in previous review, the JSON example contains flagrant formatting errors suggesting it was created by hand. Furthermore, the Chainscript includes a mapID of 56c11d0ea55773bc6e681fde. The same mapID is also used in the Stratumn documentation, suggesting copying and pasting from the docs.

The question remains **did the study actually produce any real Chainscript JSON files or timestamp even a single Chainscript file**. It's telling that the authors still haven't revealed a Chainscript file whose past existence has been timestamped. Hence, there is no evidence that the authors actually implemented their proposed "proof of concept".

Given the severity of the outstanding issues despite the number of previous rounds of review, I do not intend to review this study again. Hence, my decision to not approve this study should be considered final.

Competing Interests: No competing interests were disclosed.

Referee Expertise: data science, bitcoin, blockchains, timestamping, bioinformatics, computer science

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.

Author Response 16 Aug 2017

mehdi benchoufi, Hotel-Dieu Hospital, Paris Descartes University, France

Dear reviewer,

1) First things first, we are going to answer the serious charge you are laying at the end of the review and questioning whether “the study actually" did "produce any real Chainscript JSON files or timestamp even a single Chainscript file”. Let me dissipate any misunderstanding : we produced a JSON file and it is provided in the text.

If you look carefully at the material we furnished, the figures 4,5,6 corresponds to the data structure we got from the production experimentation and these correspond to the validated transactions. Moreover, we let as an example a JSON data structure where we listed different entries, as any documentation oriented information, and we picked up an example file and structured it accordingly to the experiment purpose. And so the HASH ID ` 56c11d0...` is not flagrant errors and is set as an example inside this merkel tree data-structure.

Of course, we furnished to the editor the production Chainscript file with the names and emails blanked out. Since you are a reviewer intervening in the health field we suppose you are aware that these kind of files contain sensitive personal data so we can not provide the very file we used. *F1000Research* requested we censor the sensitive personal data, such as names and email addresses, and so we did not publish the whole Chainscript file but after blanking out this information, it's clear to readers what has occurred.

2) We insist with the fact that we identified linking digital identities and physical entities as an important issue and as explained in our series of responses to the reviews :

- We recall that major and serious issues identified by the FDA corresponds, by a proportion of about 10% of trials, to failure to obtain written informed consent, consent documents not signed or dated, missing pages in consent document provided to subjects, failure to re-consent when new information becomes available, use of expired, non-validated or unapproved forms. This is the context we are embedding in our work.

- We want to provide solutions coherent with regards to the current state of clinical trial usages and not an idealistic one. So that, letting the investigators create keys seem not, to our point of view, the subject of major concern. Indeed, the heavy part numerous bias that entail research quality and clinical trials reproducibility are related to a posteriori reconstruction or untraceable missing information. We already furnish examples such as statistical analysis plan, definition of outcomes, inclusion and exclusion criteria, secondary effects traceability…
- besides, this issue has to be raised in “production”. We are here proposing a POC and we already suggested in the preceding round of revision that we could provide for the patients a proper generation key online interface, and this would be doubled by a key registration with a material object : USB cards are now provided by some vendors.

Despite, most of the questions we are asked are focused on Blockchain technology, one should have in mind that this is not a technology paper but medical research one.

3) Regarding the workflow that we mentioned and developed in three points, we would like to emphasise that is exactly what we have done :

- input and users transactions where recorded.
- the electronic consent process is “blockchained": the consent status is set into the Chainscript. Moreover, any version of the protocol document is hashed, versioned and bound to the consent status.
- the Chainscript file is timestamped on the Bitcoin network. Chainscript helps group the transactions and validate them as if it were one. The hashes of this data structure form a coherent and consistent group of hashes, any of them would be corrupted results in invalidating the whole datastructure . This “SideChain” approach enables us to reduce costs of transactions, which is especially useful when dealing with large clinical trials.

Best regards,
Mehdi

Competing Interests: we declare no competing interests

Version 2

Referee Report 22 May 2017

doi:10.5256/f1000research.12384.r22303

Daniel S. Himmelstein
Systems Pharmacology and Translational Therapeutics, Perelman School of Medicine, University of Pennsylvania, Philadelphia, PA, USA

In version 2, the authors updated the manuscript and responded to my review of version 1. I'd like to thank the authors for these additions, which provide a clearer picture of the trust model and proof of process. To assist in my review, I created a GitHub repository that includes a diff between versions 1 and 2.

Trust model

In their response, the authors clarify who generates the private key for a given participant:

> A participant cannot simply generate any Bitcoin address and use it to sign, because the private key is created on the server by the agent (but not saved on the server), then is sent to the email address.

I believe "the agent" refers the agent folder of the benchoufi/DocChain source code. In their proof of concept, the clinical trial investigators host the agent. Presumably, the agent could also be hosted by a trusted third party, such as Stratumn or a governing body like an Institutional Review Board.

It's crucial to note that the proof of process for participant consent requires complete trust in the agent. Assuming the agent is hosted by the investigators, then we must trust the investigators to have faithfully run an uncompromised agent. Hence, the proposed implementation provides an equivalent trust model to the current consent process. In both cases, one must trust the investigators to truthfully collect consent. Presently, we trust that investigators did not forge a participant's handwritten signature. In the proposed implementation, we trust that the investigators ran an agent that properly generated (and then deleted) a private key for each participant's email. For the time being, the later is perhaps even less verifiable than a handwritten signature. Regardless, the proposed digital identity solution requires a trusted party.

Proof of process

The authors should more clearly document the proof of process underlying their approach. The Chainscript examples (the code block and Figure 4–6) are a good start. However, Figure 4–6 are poor resolution and difficult to read. More discussion of the Chainscript format along with instructions to verify a process and timestamp are needed. For example, there is no example Chainscript JSON file provided with step-by-step instructions on how to verify or evaluate it. The Chainscript code block is littered with broken JSON syntax, so it's certainly an insufficient example. With more details, additional questions may arise. For example, is the 12-byte mapID (with a best-case attack complexity of 2^{96}) secure against preimage attacks? The manuscript doesn't appear to specify what hash algorithm is used.

Smart contracts

The manuscript is misleading regarding "smart contracts" and implies that the study proposes a smart contract enrollment protocol. Specifically:

1. Figure 1 includes a smart contract step in the workflow.
2. The abstract states "a blockchain core functionality, named Smart Contract, can help prevent clinical trial events not to happen in the right chronological order".
3. The introduction states "This makes it possible to build a Smart Contract that will be executed with the only condition that patients will only be included when the enrolment is complete".

As the authors admit in their response to my review of version 1, they "did not implement" anything related to smart contracts. Implementing a smart contract to manage enrollment is not trivial. Unless the authors actually implement such a contract, they should remove claims about its utility and applicability. Discussing smart contracts in the discussion would be justified, but it's misleading to suggest that the current proposal involves smart contracts.

Overstated blockchain usage

In their response to my review of version 1, the authors clarify that the primary achievement of the study is to create a web-based consent workflow that makes it most natural and easy to perform the proper consent process. However, the study only minimally leverages the guarantees provided by cryptography and secure blockchains. For example, the study does not achieve *trustless consent*, whereby participant consent can be provided and verified in a decentralized manner without having to trust any other parties. However, in the abstract, the authors imply the trustless & decentralized aspects of Bitcoin apply to their consent process:

> This is a distributed technology that brings a built-in layer of transparency and traceability. Additionally, it removes the need for third parties, and gives participative control to the peer-to-peer users.

In reality, the only area where a blockchain was applied is for the Chainscript timestamping. I agree this timestamping is valuable for its ability to prevent retroactive consent forgery. However, it's insufficient to verify an actual participant's identify or consent. Foremost, the use of blockchain timestamping is not sufficient to justify the grandiose claims of blockchain relevance to clinical trial consent.

In other words, the proposed consent protocol would suffer little were all blockchains to immediately disappear. The blockchain is not essential to implement more automated, web-based, and reliable consent processes. Yet the study titles itself "blockchain protocols in clinical trials" and implies that blockchains are what allows "transparency and traceability of consent". The manuscript does not adequately differentiate between speculation and the actual ways in which the study leverages blockchain technology.

For me to consider approving this study, the authors would need to drastically reduce their claims regarding the benefits of blockchain usage for clinical trial consent applications. In addition, greater clarity and focus on the specifics of their proof of concept implementation would be necessary.

Competing Interests: No competing interests were disclosed.

Referee Expertise: data science, bitcoin, blockchains, timestamping, bioinformatics, computer science

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.

Author Response 21 Jun 2017

mehdi benchoufi, Hotel-Dieu Hospital, Paris Descartes University, France

Trust model

In their response, the authors clarify who generates the private key for a given participant:

> A participant cannot simply generate any Bitcoin address and use it to sign, because the private key is created on the server by the agent (but not saved on the server), then is sent to the email address.

I believe "the agent" refers the agent folder of the benchoufi/DocChain source code. In their proof of concept, the clinical trial investigators host the agent. Presumably, the agent could also be hosted by a trusted third party, such as Stratumn or a governing body like an Institutional Review Board.

It's crucial to note that the proof of process for participant consent requires complete trust in the agent. Assuming the agent is hosted by the investigators, then we must trust the investigators to have faithfully run an uncompromised agent. Hence, the proposed implementation provides an equivalent trust model to the current consent process. In both cases, one must trust the investigators to truthfully collect consent. Presently, we trust that investigators did not forge a participant's handwritten signature. In the proposed implementation, we trust that the investigators ran an agent that properly generated (and then deleted) a private key for each participant's email. For the time being, the later is perhaps even less verifiable than a handwritten signature. Regardless, the proposed digital identity solution requires a trusted party.

Dear reviewer,

Thank you for these remarks. Indeed, you are right that, in the current setting, the “agent” hosts the entity that generates the set of keys. We have a few remarks regarding this issue.

The main aim of this implementation is to fight some specific issues related to clinical trials consent process, major concerns documented by the FDA being failure to obtain written informed consent, consent document not signed or not dated, missing pages in consent document provided to subjects, failure to re-consent when new information becomes available, use of expired, non-validated or unapproved forms. So, we simulated several stakeholders, such as investigators, institutional review boards, that played the role of trusted parties who were granted access to a dashboard monitoring all the blockchain transactions. We have considered that patients patients invention and so forging consent is hopefully a rare phenomenon in real life clinical trials, we did not prioritarily focus our attention to the very point you are mentioning and which is relevant.

However, we processed this implementation in the context of a POC and we are of course aware of the issue related to key generation. So much that, in a production setting, as discussed in the first round of revision, we would provide for the patients a proper generation key online interface doubled by a key registration with a material object, such as an USB cards to prevent from keys lost. This would enable us to benefit more broadly of the distributed nature of a “trustless” network. For sure, patients invention could still be possible but we believe that this would be a marginal phenomenon - besides, even in this case, since all the steps of consent would be timestamped on the blockchain, the entry barrier to fraud would be higher.

In the far future we envision, we would think of a standardization of some key aspects of clinical trials methods whose critical steps would happen through blockchained transactions. For example, in the model of clinical trials platforms, such as www.clinicaltrials.gov, whose information is mandatory before the study starts, a good practice would be then for patients to register on such a platform, they would then have their own key identifiers.

Proof of process

The authors should more clearly document the proof of process underlying their approach. The Chainscript examples (the code block and Figure 4–6) are a good start. However, Figure 4–6 are poor resolution and difficult to read. More discussion of the Chainscript format along with instructions to verify a process and timestamp are needed. For example, there is no example Chainscript JSON file provided with step-by-step instructions on how to verify or evaluate it. The Chainscript code block is littered with broken JSON syntax, so it's certainly an insufficient example. With more details, additional questions may arise. For example, is the 12-byte mapID (with a best-case attack complexity of 296) secure against preimage attacks? The manuscript doesn't appear to specify what hash algorithm is used.

- You can check any chainscript JSON file on the chainmap explorer : http://chainscript.io/#/chainmap-explorer.

Now, let's take as an example a sample Docchain Chain Map at http://chainscript.io/#/chainmap-explorer?application=docchain&mapId=59262a2eb446491fe9d48ecb

If one click on any of the map, for example, the first one, titled "8671b7", a JSON pops up, of which clock on the "JSON" tab, which will display the internal structure for that link. Going to the "evidence" or the "JSON" section, there is


```
"state": "COMPLETE",
  "merkleRoot": "21dd2f636a9d6b9cde1504e8fe413a65b1f2efc78d2bde1a09634cb55f0e2631",
  "transactions": {
    "bitcoin:testnet": "b39d12a54226c976795dcc85c07bd0b02feffaf92a25f48cdb356fe3aa50fcfd"
  }
```


Now if you look up the txId in the testnet blockexplorer, you will find the merkleroot in its OP_RETURN. For instance, you can try this https://www.blocktrail.com/tBTC/tx/b39d12a54226c976795dcc85c07bd0b02feffaf92a25f48cdb356fe3

- Beyond, you will find a detailed documentation of the step-by-step instructions you need in the ChainScript documentation. You'll find an explanation of the overall logic of Chainscript and the Merkel tree data- structure on which it relies, a description of the JSON structure that holds the linked sets of blockchain transactions, and the source code enabling to verify the Merkel proof is valid and so that JSON structure is consistent. It has to be precised that the source code provided is adapted to a Node.js application.

- The mapID is randomly generated, so there is no preimage attacks applicable to it. ehdiBesides, Chainscript is agnostic to the specific cryptographic scheme used to secure the process. E.g. if hashes of a certain data are stored inside the state, then the validation would equal checking hashes.
Thus, for the verification of Chainmaps, it depends on the particular choice of data stored inside a segment, that is, the Chainscript does not enforce any specific format as the `link.state` is a freeform data. (As detailed here, a state is for example a concrete implementation of a notarizing process, for example `uploading a file`, the state variable will store the uploaded name file, the user name or anything prescribed).

- As for generating linkhash, it uses SHA256 of https://nodejs.org/api/crypto.html#crypto_class_hash. The process consists in converting the JSON into a string, which is done through a regular canonical-json module. This string is then hashed.

Smart contracts

The manuscript is misleading regarding "smart contracts" and implies that the study proposes a smart contract enrollment protocol. Specifically:

1. *Figure 1 includes a smart contract step in the workflow.*
2. *The abstract states "a blockchain core functionality, named Smart Contract, can help prevent clinical trial events not to happen in the right chronological order".*
3. *The introduction states "This makes it possible to build a Smart Contract that will be executed with the only condition that patients will only be included when the enrolment is complete".*

As the authors admit in their response to my review of version 1, they "did not implement" anything related to smart contracts. Implementing a smart contract to manage enrollment is not trivial. Unless the authors actually implement such a contract, they should remove claims about its utility and applicability. Discussing smart contracts in the discussion would be justified, but it's misleading to suggest that the current proposal involves smart contracts.

We thank you for this remark, since smart contracts references appear to be far from clear. Indeed, the current state of the formulation can be misleading. The logic was to conclude the abstract section with drawing some perspectives, this is the reason for the sentence beginning with “In the future”.
So we rewrote this part, suppressed the mention from the Introduction and we referred and detailed a bit more the discussion of this matter in the Discussion section.

Overstated blockchain usage

In their response to my review of version 1, the authors clarify that the primary achievement of the study is to create a web-based consent workflow that makes it most natural and easy to perform the proper consent process. However, the study only minimally leverages the guarantees provided by cryptography and secure blockchains. For example, the study does not achieve trustless consent, whereby participant consent can be provided and verified in a decentralized manner without having to trust any other parties. However, in the abstract, the authors imply the trustless &

decentralized aspects of Bitcoin apply to their consent process:

> This is a distributed technology that brings a built-in layer of transparency and traceability. Additionally, it removes the need for third parties, and gives participative control to the peer-to-peer users.

You're absolutely right to affirm that we suppose indeed that there are stakeholders who have the root-permissions to create pairs keys are to be trusted. Indeed, the current process of clinical trials heavily relies on the existence of such stakeholders such as investigators, sponsors, regulatory agencies (FDA in the US, EMA in the EU, …) or IRBs. Depending on which stakeholders we trust, the generation of pair keys could be devoted to one of these stakeholders. For instance, if the objective is to insure mostly time stamping but investigators are trusted, the could generate the keys. If the system also wants to prevent forging consent by the investigator, then the keys could be generated by the sponsor or any other external party under the supervision of the sponsor, a regulatory agency or the IRB, and given to the patient with information documents. We thus believe our current implementation is directly usable for clinical trials as they are conducted today.

Besides, we vigorously defend the point that patients should be more involved, and we envision that, in a near future, clinical trials will let a greater part to them, especially when it comes to deal with privacy concerns. Experiments, such as the "Compare" e-cohort we are currently leading in our department, enable precisely patients to be included in a fully online patient-centric study, so that it suits perfectly to host a blockchain layer as for the consent process. As detailed above, we believe that our implementation can be adapted to ensure users can generate their own sets of keys, then benefit from the distributed nature of the blockchain network, and by then getting closer to a trustless consent process.

However, even we hope this kind of trials will become standards ones, this is not the case yet, so that our approach ensures a pragmatic usability of the current implementation of our POC by the stakeholders.

Moreover, the idea of claiming what blockchain could bring, is also related to the deep outlook of numerous bias that entail research quality and clinical trials reproducibility. In fact many issues could benefit from the blockchain technology to be better controlled, as these are frequently related to a posteriori reconstruction or untraceable missing informations. Examples are the statistical analysis plan, the definition of outcomes, or inclusion and exclusion criteria, secondary effects traceability…

From a "consent process" point of view, we measure, even with the issue of this POC's current stakeholder-sided authentication system, how much the incorruptible timestamping could drive benefits from the ground where current clinical trials are buit on : no traces other that handwritten for consents, no pairing between consents and protocol versionning... despite the issue related to key forgery, the process we are detailing prevails from a posteriori data manipulation, and this is not undoable because of the almost-inaccessible forgery of distributed ledgers. This participates of the transparency and traceability we mention.

However, we understand that filling the gap from a POC to a production implementation requires a bit of work and so we downsized the claim of the article in order to take account of the issue you raised, that we of course identified and rejected to the implementation in a real setting. We warned

the reader we did not yet implement a solution that fully exploit the distributed characteristics of a blockchain network.

In reality, the only area where a blockchain was applied is for the Chainscript timestamping. I agree this timestamping is valuable for its ability to prevent retroactive consent forgery. However, it's insufficient to verify an actual participant's identify or consent. Foremost, the use of blockchain timestamping is not sufficient to justify the grandiose claims of blockchain relevance to clinical trial consent.

In other words, the proposed consent protocol would suffer little were all blockchains to immediately disappear. The blockchain is not essential to implement more automated, web-based, and reliable consent processes. Yet the study titles itself "blockchain protocols in clinical trials" and implies that blockchains are what allows "transparency and traceability of consent". The manuscript does not adequately differentiate between speculation and the actual ways in which the study leverages blockchain technology.

For me to consider approving this study, the authors would need to drastically reduce their claims regarding the benefits of blockchain usage for clinical trial consent applications. In addition, greater clarity and focus on the specifics of their proof of concept implementation would be necessary.

We purged the text from the claims that may be considered as over-valued. For instance, we suppressed this sentence : “Additionally, it removes the need for third parties, and gives participative control to the peer-to-peer users’, “...a starting point to define a gold-standard of an open and secure informed consent collection process....”

We enforced to distinguish more clearly prospective views from the current implementation. Especially, we rejected to the Discussion section evocation of future use of Smart Contract that we envisioned or the community-based aspects of blockchain technologies, since they are pertinent in a context where the authentication keys generation process happens on the patient side.

Competing Interests: No competing interests were disclosed.

Version 1

Referee Report 11 April 2017

doi:10.5256/f1000research.11349.r21311

Daniel S. Himmelstein
Systems Pharmacology and Translational Therapeutics, Perelman School of Medicine, University of Pennsylvania, Philadelphia, PA, USA

Benchoufi *et al.* propose and implement a method for notarizing participant consent for clinical trials using the Bitcoin blockchain. At a minimum, such an approach must accomplish two cryptographic objectives:

1. provide participants with a fraud-resistant method to irrefutably consent to the terms of a clinical trial.
2. provide clinical trial investigators with a method to retrospectively verify participant consent at a given point in time.

I agree with the authors that cryptographically notarizing consent would be a major advance. If possible, there would be strong incentives, both ethical and practical, for investigators to implement and regulatory agencies to mandate such an approach.

By encoding a hash into the Bitcoin blockchain that derives from a "consent document", it is possible for investigators to timestamp a consent document and thereby retrospectively prove the existence of that consent document at a given point in time. However, I am not convinced that the study provides patients with a fraud-resistant, irrefutable method of consent. Specifically, I don't think the study provides a method for ensuring that a specific participant provided consent. In other words, can clinical trial investigators prove that a specific participant consented rather than just proving that some entity consented under the supposed digital identify corresponding to a specific participant?

The study uses digital signatures to attest that a participant approved a specific consent form. The implementation relies on bitcoin private keys to provide digital signatures. The problem is that bitcoin addresses (which uniquely derive from a private key) are pseudonymous. For example, anyone with access to a consent form could create an unlimited number of bitcoin private keys and use these private keys to digitally sign the consent form. How does one prove that a bitcoin address solely belonged to a single participant?

The generation of bitcoin private keys in this study occurs at https://git.io/vSPTE. I don't see anything in the code or manuscript that irrefutably links a participant to ownership of a given bitcoin address. Therefore, it appears to me that clinical trial investigators (or many other actors) could forge consent. In fact, the manuscript appears to concede this point with the statement:

> Each of the to-be-enrolled users ***were assigned*** a private key in order to sign data and documents, and in practice this would be used to publish their signed consent.

Linking digital identities to physical identities is difficult. However, this is a precondition to blockchain notarization of clinical trial consent. OpenPGP (the most established method for digital identity and signatures) relies on a web of trust model to link digital identities to physical identities. HTTPS relies on Certificate Authorities to link digital identities to organization identities.

Since the manuscript does not sufficiently address how it links digital and physical identities, I dug a bit deeper into Stratumn, the underlying service provider. Stratumn is a French company, which aims to "secure processes between partners through blockchain technology." Stratumn focuses on "proof of process" using a JSON data structure called chainscript. I had difficulty uncovering the implementation details of Stratumn's proof of process, as much of the available online material focuses on the implications of the technology rather than the technology itself. The most helpful resource I found was the Epicenter Podcast #159 titled "Richard Caetano & Anuj Das Gupta: How Stratumn Secures Processes." This

investigation did not answer how digital identities are linked to physical identities in Stratumn's services. The Stratumn proof-of-process white paper *does mention* identity verification under "Non-Repudiation of Source and Destination", stating:

> Non-repudiation implies that the stakeholders of the information content of each and every step should not be able to deny their involvement with the steps representing their data through the digests. The tool we will use for this is Digital Signatures.

> Both Alice and Bob need to be responsible to their respective steps in such a way they they can not repudiate their involvement if challenged. The record of their identities would be maintained by having the stakeholders digitally sign the digest of their move and then storing the signatures and public keys along with the digest in the step. The private keys will not be stored in the steps; each player hold hers separately and securely. Anyone who has access to the proof can use the public key verification to ascertain whether or not Alice or Bob can be held responsible for a step.

> In this way we enable identity management and ownership in each and every step for the proof of a process to demonstrate the Who behind each and every step.

Unfortunately, this description does not explain how digital identities are linked to physical identities. How does one know whether a digital signature is actually Alice or Bob's? Stratumn even provides a document detailing the clinical trial consent use case. However, this document does not provide an identity solution.

Conclusion

I am marking my review as *Not Approved*. **If the authors can show that it is not trivial to forge a specific participant's consent, I would be happy to revisit my decision. However, absent a reliable method to link a digital identity to a participant's physical identity, there is little benefit to cryptographic notarization of clinical trial consent.** Such an approach is only as useful as its most vulnerable step. At a minimum, the authors need to identify the trusted parties related to participant identity.

Minor points

The study could do a better job citing the relevant cryptographic literature. For example, the study cites neither the Bitcoin white paper nor the proof-of-process white paper. In addition, the study should consider referencing OriginStamp, OpenTimestamps, and Carlisle's 2014 blog post.

Figures 2 & 3 are in French. I understand that it's important to show the consent form and interface as given to the participants. However, perhaps these should be supplements with English versions in the main text.

The study states: "Smart contract: this is a contract that is algorithmically implemented and binds any change in the protocol to the patients' consent seeking renewal." However, from my understanding the study does not propose any blockchain smart contracts. Instead, the Bitcoin blockchain is only used as a timestamping service.

Positives

The study aims to replace trust with cryptography in medical research.

The study makes its source code available under a permissive open source license on GitHub (Zenodo archive).

The study understands that directly writing every document hash to a secure & immutable blockchain will be cost prohibitive, and therefore it is necessary to "group transactions", i.e. write one transactions that attests to the existence of many chainscript hashes.

Competing Interests: No competing interests were disclosed.

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.

Author Response 19 Apr 2017

mehdi benchoufi, Hotel-Dieu Hospital, Paris Descartes University, France

Dear reviewer,

Thank you for drawing our attention on the questions you raised. Our answer focuses mainly on the issue related to the binding between digital identities and physical entities.

We updated the revised version accordingly to all the questions you raised.

Target of the POC and digitale identities

POC as a response to FDA raised issues

Thank you for your constructive remarks. In fact, there are two main issues regarding the consent process. The first one is related to the quality of the process itself and the second one is related to the identity of the individual consenting. Monitoring of trials by the FDA has identified serious issues in about 10% of trials, major concerns being failure to obtain written informed consent, consent document not signed or not dated, missing pages in consent document provided to subjects,failure to re-consent when new information becomes available, use of expired, non-validated or unapproved forms (reference [3,4] in the manuscript and this link). In this POC study, we aimed at fighting these issues, where existing patients were included in a study in the presence of their physician or staff. In our implementation, we ensured that all the consent process was tracked in time all along the inclusion period, that the documents made available to the subjects were not corrupted, that they were in conformity with the current version of the protocol, and that (re-)consent was asked as many time as required. We however did not address the cases where consents were falsified by the investigating teams or where fake patients were invented for instance, which are more related to the second (identity) issue. This should be more explicit in the text, and has been emphasized in the revised manuscript.

Linking digital identities and physical entities

We then agree with the reviewer that the second issue is important in the context of a real clinical trial. This relates to the question of pairing digital identification with physical persons. In our implementation of the POC study, the link between a participant and his/her digital identity is done through his/her email address. A participant cannot simply generate any Bitcoin address and use it

to sign, because the private key is created on the server by the agent (but not saved on the server), then is sent to the email address. So the only guarantee is that the participant had access to that email address. This is pretty light, but seemed to be satisfactory given the scope and focus of the POC. Moreover, in the setting of a real online consent process, there is no chance that a patient who would not effectively consent—for instance if there were some fraudulous operation registering him/her as a consenting subject—would actually participate to the study.
However, in a production application we must implement a more secure mechanism, and we thank the reviewer again for outlining the possibilities. There are indeed several solution to secure the digital identity of participants.

First, we can mention that KYC processes are now quite widespread and there are plenty of examples where digital identities are linked to physical entities or human beings in the context of sensitive data: in most western countries the fiscal administration allows online service for taxpayers to declare their income and proceed to related operations, banking services also provides their services online such as bank transfer, account consultation. All these examples have in common that users (taxpayers, bank clients) are given a physical material, often by sending a document by regular postal service, or by giving a first card or document by hand. These documents carry an identification number. This approach could be implemented in production.

Second, even in regular off-line consent process, ensuring that the patient really signed the document is not without carrying problems. We have in mind that the patient must meet the medical doctor and receive by hand their consent document. So that, when they go back to the medical doctor with the signed document, there is no way to prove that it was signed by the patients himself or that the patient was not influenced at the time of signing the consent form. Regarding a possible implementation of our blockchained consent process in a real clinical trial, we can provide, at the moment the patient meets the doctor, authentication cards with an identification number and so strengthen the binding between the electronic signature id and the physical one. Let's mention that some bitcoin companies also provide material keys, such as USB keys, that hold the cryptographic signature, which can be unlocked by an easy-to-remember code. This can be an excellent candidate to get stronger digital-physical binding. These issues are now covered in the revised discussion.

Besides, we think that full online consent collection process raises more the issue to reach subjects that the one related to ensuring the targeted patient is really the one consenting.

Patients invention

Going further, we can summarily refer to the extreme case of patients invention. Unfortunately, there is almost no way to prevent data invention. And there are some documented case in the medical literature, fortunately very rare, where clinical trial patients and all related clinical data were invented from end to end. Let's notice here that, in the first implementation of our POC, we timestamped an extensive part of interactions between the subjects and the online email and web platform : time of the email sending, reception, time email was opened, the links being clicked on. We then validated the transactions into the blockchain, this way we could at least detect anomalies if such data appear grouped in time, so that it does not prevent from invention but higher the barrier to fraud.

Further technical improvements

On a more technical side, Stratumn's technology, via proof-of-process, provide an implementation that would allow one to create an audit trail of the the different steps that happened until the participant provided enough evidence to convince the verifier of his/her identity, which is quite an upgrade to current KYC processes, because there would be a permanent record of what happened, and the process would impose rules that must be respected to the letter (by computer code) before moving to the next step. In short, this is not a complete out-of-the-box solution to linking digital identities, but Stratumn has the tools to build one. While implementing such a verification process with the technology is possible, this was beyond the scope of the POC.

Smart Contracts

Indeed, we did not implement it in our setting, we meant to mention that Smart Contract can bind the modifications occurred in the protocol and some to be defined events on which parties can agree.
Besides, we did not detail or implement in the article all the advantages that can be derived from the algorithmic nature of the Smart Contracts: the way consent process is monitored, the way the related informations are shared between the stakeholders, the investigators and the IRB or building Smart contracts with the condition patients will only be included when the enrolment is complete or building one checking the whole consistency between the data and the blockchained proof of data, preventing from the whole hassle of gathering the documents and checking them by hand

Figures

Indeed, some figures are in french and we complied to the F1000 policy that invited us to proceed so.

Bibliography

We thank the reviewer for the precious remarks about bibliography and to have brought to the knowledge of the authors two of them, namely the one referred as `OriginStamp` and the Carlisle blogpost. We add and referenced them in the revised document.

Best regards,

Competing Interests: No competing interests were disclosed

Referee Report 04 April 2017

doi:10.5256/f1000research.11349.r19560

Mike Clarke
Northern Ireland Methodology Hub, Centre for Public Health, Queen's University Belfast, Belfast, Ireland

This is an important article, worthy of publication in F1000Research. There are some places in the article where the writing could be tidied up (e.g. references 1 and 10 are the same) but my main comments

relate to questions that prompted in my mind, which the authors might wish to address if they revise it:

Proof of concept, blockchain and the study generally

1. Is the reported study a "proof of concept" for the use in a real trial, or simply a demonstration that blockchain can be used for a series of sequential "signings"? If the latter, had that not been shown previously?

2. Are there any plans to test this in a real trial, perhaps as a SWAT[1] and to include it in Trial Forge[2]?

3. How would this system be used if patients cannot get online personally?

4. How would the system cope if someone's email addresses changes? (I raise this because I am currently locked out of my Twitter account because the email I used to set it up is no longer active following my move away from that institution.)

5. Can you reflect more on the challenges of doing online trials?

6. Do you believe that this system will be applicable to all trials, a majority or a minority? You seem very enthusiastic about the use of this system and the article might benefit from the addition of more caution about its general applicability. For example, you write "we evoked a possible improvement in the enrolment rate, by empowering patients and granting them information and control over the enrolment phase." but say little of the possible negatives (such as concerns about security of the data (see below); fear or discomfort with technology; and whether empowerment might come more from the ability to talk to a human being about the trial and the consent process).

7. Who will ensure that blockchain is future proof? Might people need to print or export a copy of the electronic record for long-term storage?

8. Does blockchain allow for "workarounds" (e.g. to move to the next step without completing the previous one if for some reason this is necessary)?

9. What do you mean by "transparency" in relation to the new system? If a potential participant thinks this means that others can see that they gave their consent, might this discourage them from joining the study?

Consent in general

10. How would this system cope with differences between the process for obtaining consent to take part in prospective research in different countries and cultures? For example, what if someone other than the patient might need to give consent?

11. Would patients be able to request that their ongoing consent is presumed without needing to be contacted again when there is a change in the trial? It might discourage patients from joining a trial if they are told that they will have to be contacted each time there is a change (especially if that change does not affect them personally).

12. What protocol changes should lead to new consent (e.g. should it only be those that directly affect the patient, or should it be those that might have influenced their decision to join?)

13. Would a patient need to be asked for their renewed consent if the change can no longer affect them? For example, if they have already completed treatment and are now on follow-up, do they need to be informed about changes in the evidence base about a side effect if they can no longer suffer that side effect?

14. Should patients be asked to consent again, or be asked if they want to withdraw? What assumption would be made if they do not reply?

15. Might it be worth discussing this new system in the context of other research into recruitment and retention (for example, as brought together in Cochrane Reviews [3,4,5,6]).

16. Is a lack of informed consent a source of bias (or might it be closer to the "truth" if patients don't realise that they are being studied) or bad ethical practice?

17. Might it be worth discussing the double standards of needing written consent for someone to receive a treatment in a trial but not needing it if they are given the treatment as part of "routine practice"?

18. How important is "written consent"? Is this unfair on difficult to reach populations who struggle to read or write?

Electronic consent

19. How would you ensure that the appropriate person "signed" the consent form if you do not see them do so? Is it easier to submit someone's electronic key, than to forge their signature?

Security

20. Might patients' concerns over the security of their data and the importance of confidentiality make them cautious about joining a trial if they had to use this system? How worried might they be because of news stories about data from banks and other supposedly secure systems being hacked and leaked?

21. Might it be worth writing something about how patients may think that paper consent forms locked in a filing cabinet are more difficult to access and make available to everyone online, than documents that are already available to the research team from anywhere on the internet.

Language

22. The words "subject" and "participant" are used to refer to people who take part in trials. I prefer to avoid "subject".

References

1. Clarke M, Savage G, Maguire L, McAneney H: The SWAT (study within a trial) programme; embedding trials to improve the methodological design and conduct of future research. *Trials*. 2015; **16** (S2). Publisher Full Text
2. Treweek S, Altman D, Bower P, Campbell M, Chalmers I, Cotton S, Craig P, Crosby D, Davidson P, Devane D, Duley L, Dunn J, Elbourne D, Farrell B, Gamble C, Gillies K, Hood K, Lang T, Littleford R, Loudon K, McDonald A, McPherson G, Nelson A, Norrie J, Ramsay C, Sandercock P, Shanahan D, Summerskill W, Sydes M, Williamson P, Clarke M: Making randomised trials more efficient: report of the first meeting to discuss the Trial Forge platform. *Trials*. 2015; **16** (1). Publisher Full Text
3. Treweek S, Lockhart P, Pitkethly M, Cook JA, Kjeldstrøm M, Johansen M, Taskila TK, Sullivan FM, Wilson S, Jackson C, Jones R, Mitchell ED: Methods to improve recruitment to randomised controlled trials: Cochrane systematic review and meta-analysis.*BMJ Open*. 2013; **3** (2). PubMed Abstract | Publisher Full Text
4. Brueton VC, Tierney J, Stenning S, Harding S, Meredith S, Nazareth I, Rait G: Strategies to improve retention in randomised trials.*Cochrane Database Syst Rev*. 2013. MR000032 PubMed Abstract | Publisher Full Text
5. Synnot A, Ryan R, Prictor M, Fetherstonhaugh D, Parker B: Audio-visual presentation of information for informed consent for participation in clinical trials.*Cochrane Database Syst Rev*. 2014. CD003717 PubMed Abstract | Publisher Full Text
6. Gillies K, Cotton SC, Brehaut JC, Politi MC, Skea Z: Decision aids for people considering taking part in clinical trials.*Cochrane Database Syst Rev*. 2015. CD009736 PubMed Abstract | Publisher Full Text

Competing Interests: I am involved in several initiatives to improve the quality and conduct of 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.

Author Response 19 Apr 2017

mehdi benchoufi, Hotel-Dieu Hospital, Paris Descartes University, France

Proof of concept, blockchain and the study generally

Dear reviewer,

Here are some responses to the questions that were raised. Besides, thank you for your remark related to the bibliography and the reference duplicate.

1. *Is the reported study a "proof of concept" for the use in a real trial, or simply a demonstration that blockchain can be used for a series of sequential "signings"? If the latter, had that not been shown previously?*

In the idea of establishing all the consent process in real conditions, we claim it is a proof of concept. We developed a complete and realistic set of interactions between fake patients and stakeholders, and we paired consent status and protocol revision through blockchain held by a single master document accounting for the whole process.

2. *Are there any plans to test this in a real trial, perhaps as a SWAT[1] and to include it in Trial*

Forge[2]?

For the moment, we have no specific plan to implement in a real trial but our POC is precisely a preparation to go further to a real setting.
We have no expertise in SWAT or in using Trail Forge platform, but it should comply with no difficulty with our implementation.

3. *How would this system be used if patients cannot get online personally?*

This is more a problem related to online consent than a blockchain related question. In situations where patients cannot get online personally, then the medical doctor should provide the consent form to the subjects by hand. Besides, let's indicate that in most countries, the written consent is legally mandatory.
There are other situations where the online access is not possible, related for example to disabilities, then either the legal representative should be given access to the online consent form, or written consent should be sought.

4. *How would the system cope if someone's email addresses changes? (I raise this because I am currently locked out of my Twitter account because the email I used to set it up is no longer active following my move away from that institution.)*

In a real clinical trial, we would set multiple ways to reach a patient : digitally, phone number, postal mail. For sure, email is not sufficient, and we would use a stronger identifying system than email, i.e. material objects storing cryptographic keys, such as a USB key. We could also build a Smart Contract triggered by a destination email error callback. Then, when this condition is met, Smart Contract would cause the other reaching methods to be proceeded. Since Smart Contract are pieces of code, this automatized processed can be customized at will.
However, although this is not the situation you are pointing to, this procedure may find a limit: there is no way to distinguish between the situation where an email has been sent without response, and the one where the email is still maintained by the institution with no access anymore for the previous account holder. But, we think this very case looks quite exceptional.

5. *Can you reflect more on the challenges of doing online trials?*

There are some challenges regarding online trials:
- people that are not in a condition to access an online platform: severe conditions, lack of consciousness, learning disability, no access to internet or people not friendly to online tools
- the current state of technologies do not allow interventional trials. However, the explosion of IoT, miniaturization could lead to imagine some specific interventional trials to be conducted online. In this respect, we mention the existence of blockchain systems specifically dedicated to connected objects.
- ensuring that the person consenting is effectively the one pretending to be: this should lead to use a strong identifier, and at minimum use KYC process (Know Your Customer) implemented to bind digital identities to physical entities in the case of sensitive data. Fiscal administration, Banks makes use of that.
It is worth noting that from a blockchain point of view, the email is by no mean a method to identify. In our settings, we generate identifiers for each patient which consists in complex cryptographic strings. It would be possible in addition of these informations stored in the local machine of the subject, to duplicate this information on a USB key or identifier cards on the model of KYC

procedure. Let's state that there are some companies providing material supports to keep the blockchain id's.

6. *Do you believe that this system will be applicable to all trials, a majority or a minority? You seem very enthusiastic about the use of this system and the article might benefit from the addition of more caution about its general applicability. For example, you write "we evoked a possible improvement in the enrolment rate, by empowering patients and granting them information and control over the enrolment phase." but say little of the possible negatives (such as concerns about security of the data (see below); fear or discomfort with technology; and whether empowerment might come more from the ability to talk to a human being about the trial and the consent process).*

Indeed, blockchain is not without carrying some issues. Our point was to put in a perspective a trend. Every new technological gap raises some fears, as the internet at its very beginning, but the overall trend is that usages have imposed. It is worth noting that users shape also technologies and their fear pushes the improvement of technologies conducting these to take more account of their needs and apprehensions.
Besides, our idea is not to rely on a technology by itself but to complete the blockchain network ability to ensure data consistency by a strong human support at any step of the clinical trial, first and foremost the consent process.
Besides, from the data security point of view, we positively think that it is much better ensured by blockchain-like technologies than the one currently used : first, because of the strong crypto-oriented transaction validation, second the distributed nature of the network prevent from the "single point of failure" problem related to centralized data collection. By the way, we can take the Bitcoin network as an example, which carries sensitive money data and which is proving to be resistant for almost ten years.

7. *Who will ensure that blockchain is future proof? Might people need to print or export a copy of the electronic record for long-term storage?*

Blockchain consist of a network of peers, anybody involved in the network storing in his computer the archive of all the history of transactions, i.e. the public ledger. So that, even if the network had to fail for one or other reason, any single node can restore the last state of the network. Moreover, if necessary, depending on the design of the blockchain implementation, we might enable the only stakeholders or if we want any participant, to export and print the copy of electronic transactions. We may have in mind that data stored are "proof of data" that can be checked to match the true data on any dedicated public website.

8. *Does blockchain allow for "workarounds" (e.g. to move to the next step without completing the previous one if for some reason this is necessary)?*

Yes, one core functionality of blockchain technologies, is Smart Contract. They allow to write algorithmically any set of conditions that modules the execution of some instructions.
But, we stress the fact the system can be "fault-tolerant" but there are no "roll-back" possibility. So, suppose that someone stores some informations but has mistaken, then he'll be able to add the new corrected information (that's what we can call a "fork"), but the first errored information is still accessible in the blockchain.

9. *What do you mean by "transparency" in relation to the new system? If a potential participant thinks this means that others can see that they gave their consent, might this discourage them from*

joining the study?

We mean by transparency that the rules are clear for anybody taking part in the process. This is the very role of the Smart Contract we already mentioned.
Besides, the perimeter of the people sharing the data can be controlled : we can decide that data can be shared by the only stakeholders, or decide that participants will be able to share access to their data with persons of trust. All this fine-grained control can be powered on the top of blockchain.

Consent in general

10. *How would this system cope with differences between the process for obtaining consent to take part in prospective research in different countries and cultures? For example, what if someone other than the patient might need to give consent?*

Differences between cultures, countries need to be tackled one by one. So that we need true implementation of clinical trials to face with those kinds of issues. I don't think there is a one general answer.
Online tools can help orienting the participant regarding to their specific situation. Moreover, we believe chat support should be provided in order to take account of specific situations

11. *Would patients be able to request that their ongoing consent is presumed without needing to be contacted again when there is a change in the trial? It might discourage patients from joining a trial if they are told that they will have to be contacted each time there is a change (especially if that change does not affect them personally).*

Indeed, there is no need to overwhelm patients with a flood of informations. However, from a general point of view, patients association often complain about lack of informations regarding the clinical trial progress, so that some calibrated informations can be delivered conveniently to the patients.
Moreover, in case of a major change in the protocol, they should be specifically targeted to get an email asking to consent again.

12. *What protocol changes should lead to new consent (e.g. should it only be those that directly affect the patient, or should it be those that might have influenced their decision to join?)*

There is heavy litterature about this. We refer it in the article: [10,11,12] in our bibliograhy and we mentionned these links detailing the protocol changes that should lead to renew the consent:
http://www.irb.pitt.edu/sites/default/files/reconsent guidance.pdf;
http://www.mayo.edu/research/documents/29-re-consent-or-notification-of-significant-new-findingspdf/
http://www.yale.edu/hrpp/policies/documents/Reconsentingguidance.pdf)

13. *Would a patient need to be asked for their renewed consent if the change can no longer affect them? For example, if they have already completed treatment and are now on follow-up, do they need to be informed about changes in the evidence base about a side effect if they can no longer suffer that side effect?*

Yes, these kind of new informations should be given to patients and require to ask for a renewed consent again, even if they are not supposed to suffer this side effect thereafter.

14. *Should patients be asked to consent again, or be asked if they want to withdraw? What assumption would be made if they do not reply?*

If patients want to withdraw, they should not be asked again.
When patients do not reply, and after ensuring by other means (emails, mail, phone call if available) that they do not provide an answer, then they should be considered has consenting because they already gave their consent.
Besides, this kind of situation can be advantageously scheduled in a Blockchain Smart Contract, that can be adapted to local legal contexts.

15. *Might it be worth discussing this new system in the context of other research into recruitment and retention (for example, as brought together in Cochrane Reviews [3,4,5,6]).*

Indeed, we might implement some Smart Contracts, checking the recruitment and retention process. So Cochrane reviewers could have an insight about whether this process was done conformally to standard procedures. However, we notice that the code of the Smart Contract should also be reviewed, so that an experienced developer should be required.

16. *Is a lack of informed consent a source of bias (or might it be closer to the "truth" if patients don't realise that they are being studied) or bad ethical practice?*

Lack of informed consent is for sure a bad ethical practice, in a strict contradiction to Helsinki declaration, Nuremberg declaration and good clinical practices.
Regarding the matter of generalisability bias, the latter is more related to the setting of inclusive criteriae than related to consent.

17. *Might it be worth discussing the double standards of needing written consent for someone to receive a treatment in a trial but not needing it if they are given the treatment as part of "routine practice"?*

In any case, the participant to a clinical trial must to sign the consent form, even he is already taking the medication for which the consent form is seeking his/her consent. At this occasion, the patients may be informed of actual informations related to the treatment, for example new side effects of a drug.

18. *How important is "written consent"? Is this unfair on difficult to reach populations who struggle to read or write?*

The written status of the consent by opposition of the electronic has not by itself more credit. However, depending on the local legal context, “written consent” is mandatory.
Besides, collecting consent of people with reading, writing or learning disabilities needs care. The person collecting the consent must assess the ability of the person to understand correctly the informations and to make a decision. The information must be given orally and to the legal representative if any. Some ethics committees allow the mediation of families or other supports at this stage.

Electronic consent
19. *How would you ensure that the appropriate person "signed" the consent form if you do not see*

them do so? Is it easier to submit someone's electronic key, than to forge their signature?

In this POC, we generated cryptographic keys for each patient. So, in this design indeed, we can't ensure that the person consenting is the person he or she pretends to be. This can be improved in different manner.
At least, using KYC standard procedures, i.e. doubling the electronic identification by one related to a physical object holding some number code. One step further would be to provide patients with an objects storing USB key storing the cryptographic signature and unlocked by a easy-to-remember id.

Security
20. *Might patients' concerns over the security of their data and the importance of confidentiality make them cautious about joining a trial if they had to use this system? How worried might they be because of news stories about data from banks and other supposedly secure systems being hacked and leaked?*

We refer to the question 6 on the notion of “single point of failure”, which answers at some level the raised issue.

In any case, patients are very sensitive to the security and the privacy of their data and this system addresses precisely this issue. Indeed, the decentralized structure of the blockchain, the involvement of anyone as a peer on the network, the ability to finegrain the data sharing perimeter, allows more control of the patients over the data workflow.

However, we are conscious that this system is very new and needs some pedagogical support. Anyway, Bitcoin is now a widespread, trusted electronic currency, available on payment platform of a wide range of websites such as Amazon, Apple’s App Store. An implementation of such processes in a real clinical trial should be the occasion to add different media support : documents, videos in order to inform patient of the benefit of using such technologies .

For the second part of the question, see the response to question 6. of the present reviewing question list.

21. *Might it be worth writing something about how patients may think that paper consent forms locked in a filing cabinet are more difficult to access and make available to everyone online, than documents that are already available to the research team from anywhere on the internet.*

Absolutely it might be very interesting.

Language
22. The words "subject" and "participant" are used to refer to people who take part in trials. I prefer to avoid "subject".

We substituted the usage of "subjects" by "participants" in the revised document.

Best regards,

Competing Interests: No competing interests were disclosed

Discuss this Article

Version 1

Reader Comment (*Member of the F1000 Faculty* and *F1000Research Advisory Board Member*) 02 Feb 2017

Pierre-Marie Lledo, Perception and Memory Laboratory, Institut Pasteur, France

As clinical research has to face an ongoing lack of trust, this article comes at a right moment to address key issues such as transparency, reproductibility and eventually a more reliable methodology. Blockchain technology provides interesting proof of data and therefore a trustworthy environment in order to exchange clinical data. It can lead to a substantial breakthrough which will help to set up health communities with common ethics and patients empowerment.

Competing Interests: No conflict of interest.