MEDICHAIN

Legal Disclaimer

PLEASE REVIEW CAREFULLY THE PRESENT SECTION "DISCLAIMER OF LIABILITY". IF YOU HAVE ANY DOUBTS AS TO WHAT ACTIONS YOU SHOULD TAKE, WE RECOMMEND THAT YOU CONSULT WITH YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S). No part of this Whitepaper is to be reproduced, distributed or disseminated without including this section "Disclaimer of Liability".

The information set out below may not be exhaustive and doesn't imply any elements of a contractual relationship or obligations. The sole purpose of this Whitepaper is to present MediChain and MCU tokens to potential token holders in connection with the proposed token sale. Despite the fact that we make every effort to ensure the accuracy, up to date and relevance of any material in this Whitepaper, this document and materials contained herein are not professional advice and in no way constitutes the provision of professional advice of any kind. To the maximum extent permitted by any applicable laws, regulations and rules, MediChain doesn't guarantee and doesn't accept legal responsibility of any nature, for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising from or related to the accuracy, reliability, relevance or completeness of any material contained in this Whitepaper. Further, MediChain does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity, person, or authority, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this Whitepaper. You should contact relevant independent professional advisors before relying or making any commitments or transactions based on the material published in this Whitepaper.

This Whitepaper is not subject to any legal system and is not governed by any law. No regulatory authority has examined or approved of any of the information set out in this Whitepaper, and no such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this Whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

You don't have the right and shouldn't buy MCU tokens if you are (i) a green card holder of the United States of America, or (ii) a citizen or a resident (tax or otherwise) of the United States of America, Puerto Rico, the Virgin Islands of United States, or any other possessions of the United States of America, or People's Republic of China, or person of those states or (iii) a citizen or resident (tax or otherwise) of any country or territory where transactions with digital tokens and/or digital currencies are prohibited or in any other manner restricted by applicable laws. Purchased MCU tokens cannot be offered or distributed as well as cannot be resold or otherwise alienated by their holders to mentioned persons. It is your sole responsibility to establish, by consulting (if necessary) your legal, tax, accounting or other professional advisors, what limitations, if any, apply to your particular jurisdiction and situation, and ensure that you have observed and complied with all such restrictions, at your own expense and without liability to MediChain.

MCU tokens are not and will not be intended to constitute securities, digital currency, commodity, or any other kind of financial instrument and have not been registered under relevant securities regulations, including the securities laws of any jurisdiction in which a potential token holder is a resident. This Whitepaper is not a prospectus or a proposal, and its purpose is not to serve as a securities offer or request for investments in the form of securities in any jurisdiction. However, in spite of the above, legislation of certain jurisdictions may, now or in future, recognize MCU tokens as securities. MediChain does not accept any liability for such recognition and/or any legal and other consequences of such recognition for potential owners of MCU tokens, nor provide any opinions or advice regarding the acquisition, sale or other operations with MCU tokens, and the fact of the provision of this Whitepaper doesn't form the basis or should not be relied upon in matters related to the conclusion of contracts or acceptance investment decisions. This Whitepaper doesn't oblige anyone to enter into any contract, to take legal obligations with respect to the sale or purchase of MCU tokens, and to accept any crypto currency or other form of payment. Potential owners of MCU tokens are advised to contact relevant independent professional advisors, on the above matters.

Certain statements, estimates and financial information contained herein constitute forward-looking statements or information. Such forward-looking statements or information involve known and unknown risks and uncertainties, which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements. Further, all examples of calculation of income and profits used in this paper were provided only for demonstration purposes or for demonstrating the industry's averages. For avoidance of doubt, nothing contained in this Whitepaper is or may be relied upon as a guarantee, promise, representation or undertaking as to the future performance of MediChain and/or MCU token, and/or promise or guarantee of future profit resulting from purchase of MCU token.

MCU tokens cannot be used for any purposes other than as provided in this Whitepaper, including but not limited to, any investment, speculative or other financial purposes. MCU tokens confer no other rights in any form, including but not limited to any ownership, distribution (including, but not limited to, profit), redemption, liquidation, property (including all forms of intellectual property), or other financial or legal rights, other

than those specifically set forth below. While the community's opinion and feedback can be taken into account, MCU tokens do not give any right to participate in decision-making or any direction of business related to the MediChain service.

Section that immediately follows this disclaimer, is written solely for the good faith purpose of saving your time, and in no case should be understood as recommendation not to read the whole Whitepaper.

English language of this Whitepaper is the primary official source of information about the MCU tokens, any information contained herein may from time to time be translated into other languages or used in the course of written or oral communications with customers, contractors, partners etc. In the course of such translation or communication some of the information contained herein may be lost, corrupted or misrepresented. In the event of any conflicts or inconsistencies between such translations and communications and this English language of Whitepaper, the provision of this English language of Whitepaper as original document shall prevail.

MEDICHAIN

Saving lives with Medical Blockchain.

Knowledge is of no value unless you put it into practice.[1]

Preamble

I'm Dr Mark Baker, Oxford PhD, Cancer scientist & Big Data specialist with over 50 million people using systems that I've developed. I'd like to give you a use-case that explains one slice of what we want to do.

Over 8.5 million people die from cardiovascular disease, stroke and hypertension each year, UNNECESSARILY. Published data in the British Medical Journal shows that this is the number of lives that we could save (mainly in 35 year old+ males) by implementing known, existing, methods of cardiovascular screening through MediChain. And that is just ONE example. So MediChain, linked through our API to one of our partner smart monitoring solutions could actually save your life (and save you about 6-8 years of suffering which lies between a first, unexpected cardiac event and death). Or the lives of loved ones.

This is why I've built a world class team to create a blockchain & AI tool to crack this and other huge but solvable problems.

Abstract

MediChain is a Medical Big-Data Platform. Our proposed system allows patients to store their own medical data off-chain in an appropriate geographic domain.

It not only allows them to share it with doctors and specialists anywhere, regardless of the payer network or EMR used, but also allows them to share it anonymously with scientists working to develop treatments and cures, providing Big Data to revolutionize treatment development and monetize via pharmaceutical companies, researchers and insurers.

Patients, doctors, and hospitals could put data into a compliant cloud which becomes part of the MediChain ecosystem[2] and the blockchain stores pointers and

[1] Anton Pavlovich Chekhov, playwright and short writer, 1860-1904

[2] Essentially big data - every piece of medical data they have for the patient including medical images etc.

rules on usage and anonymity, while the data itself is stored off-chain in a compliant cloud.

Patients could access their data at any time and allow other doctors and hospitals to access selected parts of the data transcending individual electronic medical records systems.

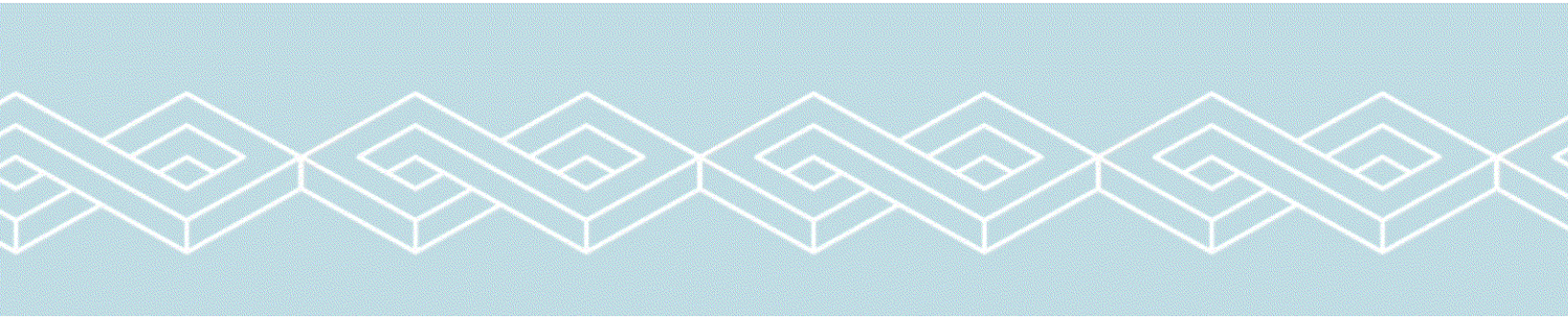
Researchers and Pharmaceutical companies would access the data as big data in fully anonymised form and use AI from our ML modules and our toolkit. It is monetized by the ability for patients to voluntarily give anonymised access to untampered data to pharmaceutical companies, researchers and insurers. Potentially it may also be used for prescription management.

Its unique architecture allows fast access and small downloads to make it practical for everyday medical use. The protocol is based on smart cards (optional), Homomorphic encrypted access rules tables, json data formats, lightweight and strong cryptography and blockchain technology, which brings enhanced transparency and reliability in medical data exchange at every level, from devices to EMR to unprecedented opportunities for privatised big data sharing.

The protocol enables connections between patients, service providers, medical researchers and AIs located anywhere in the world, regardless of systems used so long as the systems can work with the almost universal and open json format.

By improving patient data sharing and availability, and being open to add to any existing system or be managed automatically by doctor or by patient, MediChain aims to allow better conditions for all parties, creating a better way of handling patient data than anything available today.

By including different levels of access in rules MediChain seeks to neutralize the patient's risk and increase their benefits.



Contents

Context

Medical information is dispersed and inaccessible, not only to researchers, decision makers and developers of treatments, but to doctors and patients themselves. Even when it is recorded, data is siloed in multiple EMRs, paper notes, prescription records, multiple smart devices and specialist databases[3]. For example, Mike Orcutt of MIT Technology Review tells us that there are 26 different electronic medical records systems used in the city of Boston alone, each with its own language for representing and sharing data. In the legacy system, critical information is often scattered across multiple facilities, and sometimes it isn't accessible when it is needed most[4]. This is a global reality, costing money and lives. We see it as a problem tailor-made for a blockchain working with off-chain big data solutions to help solve.

[3] See http://www.reuters.com/article/us-health-hipaa-charts/patient-cant-always-access-complete-medical-records-doctors-say-idUSKCN0YE2PY

[4] See https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/

MediChain

Description

Whenever any data is gathered about a patient, by device or medical professional, dispensing a prescription or even purchase of a non-prescription medication, the patient (through an app) or the device would get a chance to have a reference or "pointer" added to an Ethereum blockchain—a decentralized digital ledger. So the blockchain is an index to storage and it contains the hashes that validate the offchain data.

Instead of payments, this blockchain ecosystem would record critical medical information off-chain, indexed by a virtually incorruptible cryptographic database, maintained by a network of computers, that is accessible to anyone running the software and has the patient's permission to access the specific cryptographic keys.

Every point at which a doctor logs on the blockchain (or the patient logs on for themselves with their smartcard, giving them control of their own data) would become part of a patient's off-chain record, no matter which electronic system the doctor was using—so any caregiver

could use it without worrying about incompatibility issues.

In this way, blockchain technology can give patients more control over their information and streamline the exchange of medical records in a secure way, protect sensitive data from hackers, and make sure that patients benefit from sharing information. A custom-built “healthcare blockchain” will herald an industry-wide revolution in medical records at a far deeper level than has been postulated previously.

Specific rules can be flexibly added to the protocol enabling it to radically improve health care, while adding value along the whole chain. The rule network is flexible and extendible and will facilitate the exchange of complex health information between patients and providers, between providers, and between providers and payers, remaining secure from malicious attacks and giving previously undreamed of control over privacy.

MediChain will provide innovation in electronic medical records (EMRs) by providing a free-to-integrate open source API to add MediChain to any EMR without regulatory barriers. MediChain is a solution tuned to the needs of patients, the treatment community, and medical researchers. It adds a novel, decentralized record management system for EMRs that uses blockchain technology to manage authentication, confidentiality, accountability, and data sharing while storing data off-chain in a secure cloud. The modular design integrates with providers' existing, local data-storage solutions, facilitating interoperability and making our system convenient and adaptable.

Global, blockchain-based patient identifiers, which can be held in patient held smartcards[5] can amalgamate hospital records as well as data from other sources like employee wellness programs and wearable health monitors, and seamlessly weld together the components of current digital systems treating them as additional off-chain data stores.

Global Market Size

The average cost of developing a new drug is $2.6 billion US taken over 106 samples and 10 companies. The annual development budget in the US is $157

[5] For Smartcard in this document and throughout MediChain we mean ISO 7816 CPU/MPU cards with 32 bit Public Key with optional 13.56 ISO 14443 contactless function for less secure interaction types (such as cached prescription information) moving on to Vault Cards with biometrics and one time passwords

billion dollars per year. Founder Mark Baker has first hand experience in this sector doing big data analysis for a crucial part of the development of a highly successful drug as well as big data experience as CTO in a major predictive analytics player.

Ultimately, the potential medical big data market is a substantial portion of the future drug development market.
In addition, and acting as an enabler, Transparency Market Research's study of the Electronic Health Records (EHR) Market [6]values the global EHR market at $15.56 billion USD (Growing to $23.98 billion USD).

Although we could try to monetize that, it makes more sense to aim to bring substantial extra value to that market by creating an acceptable system to monetize data in the EHRs while benefiting patients and doctors.

This represents just part of the value of the MediChain data set as it excludes fine grained big data (e.g. out of wearables, diagnostic devices and hospital and specialist databases) and excludes additional value created by the value of data to insurers and pharmaceutical companies, which can be conservatively estimated as 20% of the current annual spend on Pharmaceutical research of 157 billion U.S. dollars[7] [8].

What is the plan?

Working from our existing demonstrator, MediChain system has been developed with Hyperledger Fabric for speed and scalability with offchain data stored in secure clouds in appropriate regions. We already have neurological and pain control databases and collaborations and we are adding a number of medical specialities such as epilepsy and rheumatology and specific diagnostic devices. We are working on advanced AI integration with Wolfram Alpha & Mathematica and the next phase will be building up the chain data warehouse through an open access API and medical partnerships. MediChain will then be made publically available through the API and through partners for data acquisition. Then an exchange will been developed to allow secure controlled anonymized data access to patient data.

[6] Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2014 - 2020

[7] Total global pharmaceutical research and development (R&D) spending from 2008 to 2022 (in billion U.S. dollars) https://www.statista.com/statistics/309466/global-r-and-d-expenditure-for-pharmaceuticals/

[8] These form a major part of the costs of clinical trials, which the Tufts Center for the Study of Drug Development has estimates at $2.6 billion per drug.

Philosophy

The underlying philosophy of MediChain is that all personal data has value which should belong, in the first instance, explicitly to the patient. The patient can decide if they want to sell it in an anonymized form, for example to to insurers or pharma companies, but that's for them to decide. According to Seidenberg in Wired, 85 percent of smartphone buyers expect to access personal health data on their devices[9]. Optimizing the MediChain blockchain to be usefully accessible in that way is a key to success.

Utility Tokens

What are the Tokens?

MediChain Utility Tokens (MCU) represent the data in the MediChain system. There is a fixed number of tokens, so the greater the value of the data in the system, the greater the value of each token.

The big data in the system will be greater than the sum of its parts, as it will allow computational analysis to reveal patterns, trends, and associations that could not be discovered otherwise, so the value of the data will increase in a non-linear way as data is added.

MediChain tokens will be integral to medical data sales and medical services sales, but in general will be used in the background, within the MediChain system. This means that patients can simply pay money for services; healthcare providers, algorithm providers and data processing providers can simply receive money for their services; and data purchasers, i.e. pharmaceutical companies and anyone else buying data, can simply pay money for data.

In the background, in the MediChain system, tokens will be used to purchase digital medical services for patients, and to purchase anonymised patient data for data purchasers.

How are tokens used when cash is paid for data or services?

Example of pharmaceutical company buying data:

Step 1: Pharmaceutical company wants to undertake a preliminary study and needs a relatively small amount of data.

[9] You Should Share Your Health Data: Its Value Outweighs the Privacy Risk https://www.wired.com/2014/11/on-sharing-your-medical-info/

Pharmaceutical company pays money to MediChain.

In the background this purchases tokens that token holders have listed for sale, starting with the lowest priced tokens. (Token holders place tokens on the MediChain internal exchange, with a value at which they want to sell. Some tokens may be priced at a low value whereas others will be priced at high value.) The appropriate number of tokens is sold for the price of the data.

At this point, token holders who wanted to sell when the token price reached anything up to a certain level have sold tokens. (The order of whose tokens sell first when equally priced will be determined algorithmically.)

These tokens then purchase the data from MediChain for the pharmaceutical company, so MediChain now owns the tokens (and can set a selling price), and the pharmaceutical company gets the data.

Step 2: Pharmaceutical company gets interesting results in the preliminary study and now wants to undertake a full scale study, needing a large amount of data.

Pharmaceutical company pays much larger amount of money to MediChain.

In the background this purchases tokens that token holders have listed for sale, starting with the lowest priced tokens. Because a large amount of data is being purchased, the number of tokens sold will be greater, and will include higher priced tokens as well as any remaining low priced tokens, to make up the appropriate amount for the data sale.

At this point, token holders who wanted to sell when the token price reached anything up to a certain higher level have sold tokens.

These tokens then purchase the data from MediChain for the pharmaceutical company, so MediChain now owns the tokens, and the pharmaceutical company gets the data.

In summary a pharmaceutical company wanting to buy a relatively small amount of data in order to undertake an initial investigation can get it at a relatively low price, which fits their need for an initial investigation, as the first tokens involved in a data sale will be the lowest priced tokens. If the results of the initial investigation suggest that a fuller investigation is worthwhile and worth investing in, the company will then purchase a larger amount of data. This will be beyond the number of low-priced tokens, and they will have to buy high

priced tokens as well. The overall price they pay per token on average (per amount of data) will be much higher than it was in their preliminary purchase, but again fits their need as they already have the preliminary results and know that (1) the full scale investigation is worthwhile, and (2) the value of the big data they want is worth more the sum of its parts.

There will always be enough tokens available for them to buy as much data as they want to.

MCU Utility tokens can be purchased via the platform during the tokens sale. A rule of thumb is that initially, the data from each consultation or piece of data is given a value in MCUs equal to buyer cost of the consultation in US dollars. Over time the value of data adjusts according to token availability, different data types, diseases, patient demographics etc., to reflect the buyer's market. Data is available (subject to rules and anonymization) through one or more marketplaces to buyers.

Because the tokens represent the data in the MediChain system, and because there is a fixed number of tokens, the more the data is worth to buyers, the greater the value of each token. Furthermore, because big data is worth more than the sum of its parts, the value of the data, and therefore the token, will increase in a non-linear way as data is added.

Token Utility

Utility Tokens (MCUs) can be used for:

Research Program Voting

MediChain funds and tokens support the creation of research grants particularly aimed at academic institutions, healthcare networks, universities and scientists to gather high-value big data to MediChain (and the research community). MediChain Utility Tokens are used to vote on determining the focus of future research. Voting options are determined by internal and external domain experts.

Institutional Medical Data Services (including Diagnosis)

Institutions holding utility tokens will be able to use their tokens to pay for or purchase any appropriate digitally transmitted medical services, such as diagnostic services.

Research Medical Data Services

Researchers will be able to access data depending on the rules set by the patients uploading the data. From the researcher's point of view it becomes primarily big data. An academic researcher may be able

to access the data set either freely or for a nominal fee paid by the research grant (like 12 months access for $10K worth of tokens). Their findings when published will stimulate further interest in MediChain as a research resource. A researcher or research group in a pharmaceutical company may be able to do a shallow sweep through the data to look for epidemiological trends and correlations for maybe $100K or subscribe to do that. After that they would typically pay much more (up to many millions of US dollars) for a full, in-depth data set suitable as part of a new drug discovery or validation. (For more detail, see above under 'How are tokens used when cash is paid for data or services?' and below under 'Example of how data may be sold for tokens'.)

Personal Medical Data Storage and Transfer

All patients regardless of whether they are utility token holders will get to store pointers to their data without charge on the chain ecosystem[10]. Utility token holders with more than 100 tokens will be given smart card access to their own data once it is implemented, probably in year two.

[10] It is called an ecosystem here because there may, ultimately, be more than one chain involved.

Personal Medical Data Services

Individuals holding utility tokens will be able to use their tokens to purchase any appropriate digitally transmitted medical services, such as diagnostic services from institutions participating in the system.

MCU Discounts

MCU Tokens will be usable for discounts for a range of digital services as well as purchase of compatible devices which may include Fitbit products like the Fitbit Alta HR, AliveCor Cardiac Monitors like the Kardia, Apple Watches like the The Apple Watch Series 3 and related healthkit products from partners. MCU Token discounts will also be used for discounts on medical services which may include consultations and prescriptions in applicable domains.

Example of how data may be sold for tokens

A client company, typically a pharmaceutical company, wants to purchase data. Although there may be an account manager working with them, this is not essential and they can create an order through an API, providing a request on required set of metrics (patients disease, age range, sex etc), the available amount of medical records in the

ecosystem can be received by API request, thus the price of data can be known in advance.

When the payment for the data purchase service is done, MediChain company converts received fiat funds into tokens and transfers them to a smart contract. The smart contract receives tokens with an attached message on an order requirements set of metrics, connects to a private API, receives addresses and hashes of patients whose data should be added to an order delivery result, integrates data collection to a single package (which will be delivered to a purchaser), after that order delivery is made to a purchaser.

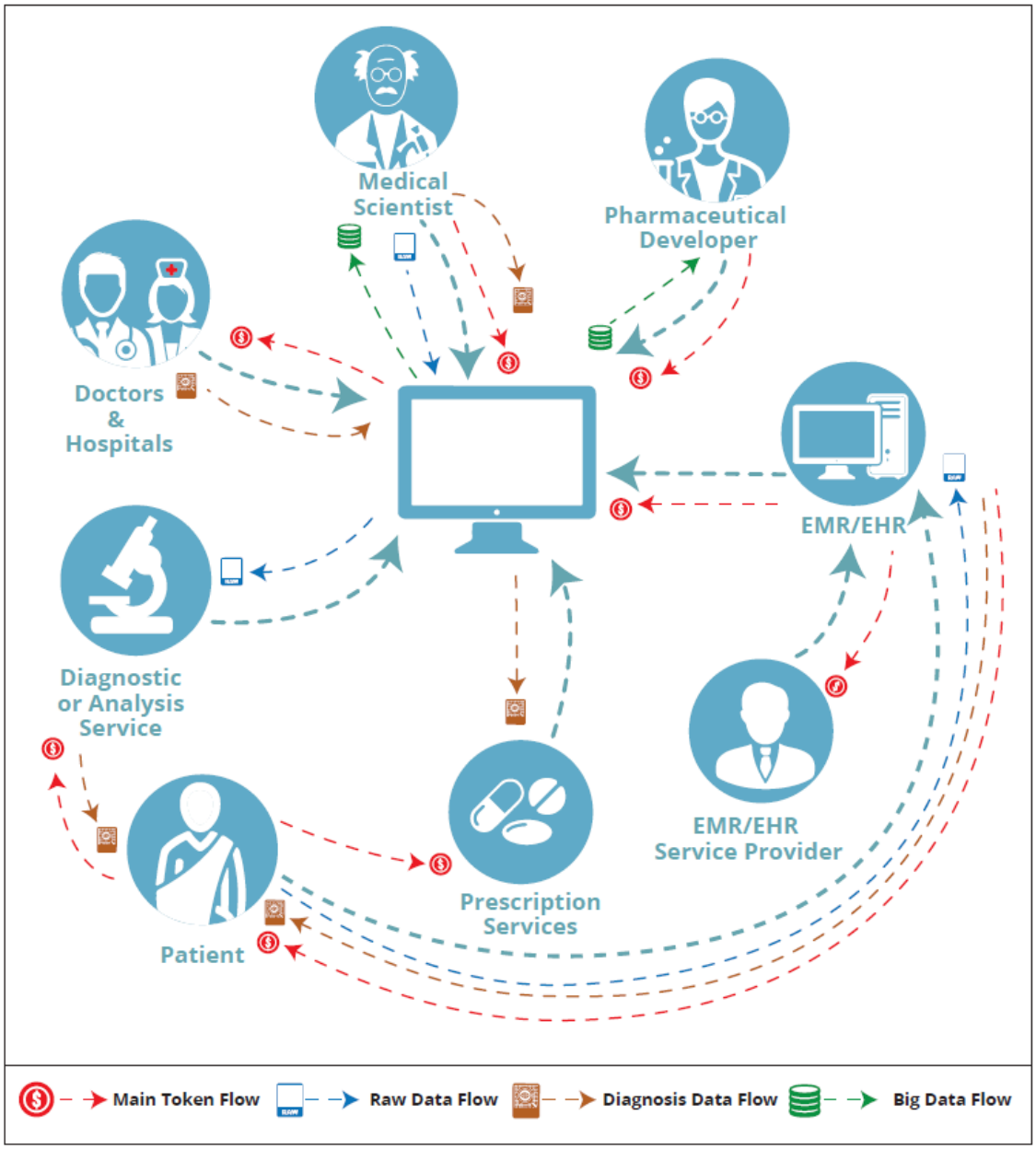
The patients' accounts whose data was purchased in total receive some portion of tokens[11] These tokens are distributed proportionally between: patients and clinics or other providers who added this data to the system database, the proportion of tokens distribution should be designed as well with MediChain help[12]. MediChain company receives the rest of the tokens, which are sent by smart contract to a service provider address..

When this data is sold, the patient gets a proportion of the revenue (again according to rules) through the MCU ledgers. Broken pointers will be cleaned from the system automatically following specific programmable rules.
In addition when a patient loads data pointers to MediChain they can tender clinicians, providers and algorithms to perform analyses and diagnoses on this data. This can be done anonymously. The results of these are uploaded to the blockchain (with suitable anonymizers). These can be accessed by patients paying using MCUs, which can be bought with fiat currency or BitCoins, paying a proportion to the clinician, provider or algorithm developer.

The figure following shows, in simplified form, how tokens and data flow around the MediChain ecosystem.

[11] E.g. 20% - subject to specific factors in the token economy.
[12] In a variation of this MediChain will seek out patient sets to order so that big data clients can essentially pre-order data which medichain establishes the contracts to obtain.

Figure: How the Tokens are Used.



This figure excludes use of tokens to pay in whole or part for services for the sake of simplicity.

We have outlined a number of other use cases later in this document. There are many classes of data that can exist in the chain(s) but understanding some of them can help understand the potential of the system.

i Raw User Data

The user's raw medical data (scans, EMR records, lab test results) belongs to the user. In addition to the value that it has to the user, it has financial value which the user controls. This is stored on a secure standards compliant cloud and indexed by a decentralized, trustless system to maintain its integrity. There may be some sort of financial or token transaction between the user and the provider of the diagnostic device to pay for the generation of that data (e.g. to pay for a scan, BP measurement, blood test etc). That is secondary. In any case the raw data belong to the user in exactly the way that bitcoin belongs to the purchaser. (The same could apply to your personalized behavioural data.) It's indexed by a blockchain, because on a large scale we are looking at multiple providers, data integrity for clinical trials, FDA approval etc. This has the same issues of integrity around it as currency.

ii Interpretations and diagnoses

These come from the user data and are provided by third parties such as doctors, specialists, algorithms and AI. Ownership is shared between the original user and the body providing interpretation. If the user shares with, say Harvard Medical School, they might allow it to be free for publication and research. If they share with a digital diagnosis company they might pay in coin to get a further interpretation of their raw data. Combined with the data (i) above this information at first replicates and later replaces conventional EMR systems.

iii Structural Data

This can identify data sets within the blockchain ecosystem[13] which are of use to treatment developers, academic scientists, or insurers, anonymously through cryptographic hashes.

Social Benefit

Population-based de-identified patient data has already produced advances against WHO top ten diseases such as obesity, diabetes, hypertension, and heart failure. Population data lets researchers

[13] The ecosystem includes all blockchains and offchain data

tackle the big issues in medicine. By patients opting in and sharing their data, they promote the research breakthroughs that can one day improve their own health and help people who are suffering from similar health issues. Where there are commercial interests involved, such as drug development, the same applies, but pharmaceutical companies pay for the data and patients are paid for their contribution.

What about emergency access to medical data in MediChain?

In an extended version of MediChain, information that is normally available to doctors in an emergency needs to be readily accessible even if the patient cannot give consent. Access needs to be customer defined with defaults consistent with current practice. It seems likely that most patients' doctors will have access to the same level of records that they let them have now. Because there are multiple rules, the emergency services will have access to the level that the patient would normally grant them now (e.g. diagnostic levels). Neither of those levels would have mass access to raw data that might be useful to pharma or insurers and if necessary anonymity could be preserved while allowing access to the complete medical record.

What are the use of funds?

The funds are used to develop and promote the MediChain infrastructure and API and carry out the initial population of the chain with data which gives the chain market value. Promotion will be through wearable, desktop and kiosk devices including Apple Healthkit, Healmet Inc and through the Scripps Medical Research Center. A proportion of the development and promotion funds will be used to mature and integrate hardware used with the MediChain system including Smart Card ID systems and IoT devices.

What is the development roadmap?

The MediChain system is developed with hyperledger fabric framework in the next 6 months partnering closely with WSGR and Flat Iron Technologies, LLC to ensure HIPAA compliance, to alpha launch.
Specific partners, whom we are in communication with to start the chain population, include pain control and neurological imaging and additionally three possible national specialist networks in Epilepsy, Rheumatology and Pediatrics. In addition, we have major EHR partners Cerner, Epic and OpenEHR. From there, and

within 12 months, MediChain is made publically available through the API and through partners for data acquisition. By month 18, an exchange will have been developed to allow secure anonymized data access.
The technical founder has executed roadmaps of similar complexity several times before and has access to team and resources used for these previously if required.

How will the organization interact with the token once it hits the market?

Tokens will be fixed in number. They will be used by MediChain for research project voting.

Is anyone holding on to token supply beyond the pre-sale?

The holding of tokens is outlined in the token allocation section. 46.5% of tokens will be released, 6.5% in the presale, 40% in the main sale. The soft cap for the presale and main sale, combined, is 2 million MCU. The are no plans for further releases of tokens to be made. Residual commitments can be settled with the for-sale or partnership pools.

HIPAA, FDA 510(k), IEC 60601-1 and ISO 13485 compliance.

The easiest, fastest way to HIPAA compliance is to store all off-chain data in a pre-certified HIPAA compliant cloud[14]. It would then just be necessary to get our interaction audited. Our quotes for this end-to-end process are approximately two weeks. We will aim to have an additional AES-256 layer on top of any third party solution to further secure data.
Ongoing standards compliance is essential, but we can add considerable value to the blockchain using our partner's existing compliance. Immediately post funding, MediChain will put in place a specialist HIPAA, FDA 510(k), IEC 60601-1 and ISO 13485 compliance officer who will check that everything going into the chain is not just compliant, but correctly certified.
We anticipate that initial data will be coming from the UK where we can get the huge required data sets quickly and at no cost. These are typically of a similar quality to the best US data, and are large enough to be of substantial value to

[14] E.g. https://www.skyhighnetworks.com/cloud-security-blog/top-5-hipaa-compliant-cloud-storage-services/

pharmaceutical companies worldwide. Solutions can be delivered to the US population and credibility can be established for US companies even before the databases fill with US-derived data. In the US, HIPAA has over 157 requirements and it is most effective to address these post-funding as we need individual HIPAA compliance both for the new corporate entity (added by entity location), for each class of data (which we will need to certify as we access each source), for each involved individual (who can only be trained after hiring post funding), and for the mass storage protocols which are yet to be built.

This is why we are not offering a clinical service or uncertified device at the time of the token sale. There are certainly very serious issues around doing that prior to certification. Everything that goes into the medical ledger will be fully certified and categorised by region of validity.

Architecture

In order for MediChain to avoid the scaling limits that other blockchains, we will be refining the normal offchain data storage model as we develop the solution.

We will use a pilot system as a proof of concept.

We have further solutions under development to make the system significantly faster and more than keep up as we add records and patients.

When considering the type of scenario we wish to avoid, a typical high-grade Bitcoin network client stores the entire transaction history, and this record for bitcoin, in 2017, was already 100GB[15]. The more transactions processed on the network, the faster the size grows and this easily outsteps Moore's law.

In addition to the need to store a large chunk of data, the data has to be downloaded as well. This is not practical if hundreds of gigabytes need to be downloaded by either doctor or patient, a process that could take many days.

If each network node does the same thing, then obviously, the bandwidth of the entire network is the same as the bandwidth of one network node. For the Bitcoin network, Alexey Malanov claims that the network is capable of processing a maximum of seven transactions per second — for the millions of users worldwide. And that Bitcoin-blockchain transactions are recorded only once every 10 minutes.

This simply is not going to work for normal doctor-patient interactions, far more medical devices syncing daily or even more frequently.

[15] The same as the full capacity of a cheap laptop's or the most advanced smartphone's storage.

What's more in blockchain, in order to increase payments security, it is standard practice to wait 50 minutes more after each new record appears because the records regularly roll back.
This is why you don't buy a snack using bitcoins. Unless you want to stand in line for an hour at the store. For sequenced medical procedures in a clinic or hospital that will not be workable either.

Malanov claims that Bitcoin is used by just one in every thousand people on the planet and says that given the transaction-processing speed, significantly increasing the number of active users simply isn't possible.
To overcome this the MediChain architecture needs to take a better approach. Starting with Hyperledger Fabric we will move on to data being divided into index blockchain(s), horizontal sector blockchains with each chain holding data for a specific set of ailments[16]. We are also considering how to implement vertical patient blockchains, the latter allowing users to locate the former across the cloud.[17]
Thus each disease would have its own blockchains relevant to a specific ailment and research community, which could be mined in that community by academics and companies with an interest in that particular set of ailments.
Implementing the horizontal blockchains, each patient-doctor interaction would therefore only have to access one repository per consultation.
Time for download of repositories would be reduced and typically specialists would have those repositories. Anonymity would be maintained by repository access in the first instance the user ID being hashed with a strong (let's say 1024-bit sha) hash and a salt code which is either weak (pin), specific (biometric) or strong (e.g. 3FA). This might develop over time. Optionally we would allow additional encrypted user identification and an optional distributed anonymous proxy service (which can be third party to decentralize).
There are still shared databases and require multiple access, it is essential that

[16]As defined under the World Health Organization International Classification of Health code system (i.e. the ICD, ICF & ICHI codes)
http://www.who.int/classifications/icd/en/
http://www.who.int/classifications/icf/en/
http://www.who.int/classifications/ichi/en/

[17] In fact the whole Ethereum network accumulated 200GB of history data in the blockchain, within two years of launch and six months of active use. We can see that a universal medical blockchain's life span is limited to about a decade, if we don't follow to architecture outlined. Thus we plan to create a system technically based on Ethereum, but one that does not piggyback it.

there is interaction between the transactions, and that we still see disintermediation of patient data. So a blockchain approach is still the best way. Local data may also contain complete or fragments of other user's blockchains striped across multiple users storage, which are stored for backup.

Localization

Blockchain is decentralized by nature, but in almost any country there is a law that regulates physical location of personal data of citizens of that country. However, by only having the pointers on the chain, that becomes irrelevant. The data itself will be AES 256 encrypted[18] and located in cloud services in the appropriate national domain.

[18]While separate action needs to be taken to protect against side-channel attacks, breaking a symmetric AES 256-bit key by brute force requires 2^{128} times more computational power than a 128-bit key. Fifty supercomputers that could check a billion billion (10^{18}) AES keys per second (if such a device could ever be made) would, in theory, require about 3×10^{51} years to exhaust the 256-bit key space. This is relevant because there are concerns that while codes of this sort may be secure today users want to be sure that they will remain secure in the future too.

Building from Experience

MediChain will give patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties, it manages authentication, confidentiality, accountability and data sharing—crucial considerations when handling sensitive information. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable. MediChain thus enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata. We regard this as a proof of concept through which we analyze and develop our approach. Allowing customers like pharmaceutical companies to scan the databases, look for correlations for a reduced fee, and then pay for the full data if they see useful correlations would be a huge positive feature that we intend to implement. However, security is a major issue. According to Humer & Finkle of Reuters, an individual's medical record is worth more

to hackers than their credit card[19], while Schlesinger & Day of CNBC reports that 4.5 million patients had their records compromised by hackers accessing one of the largest U.S. hospital operators, Community Health Systems Inc[20].

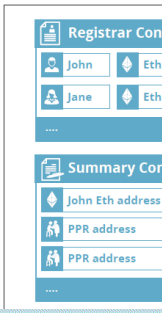
System Implementation

Overview

The block content represents data ownership and viewership permissions shared by members of a private, peer-to-peer network. Blockchain technology supports the use of “smart contracts,” which allow us to automate and track certain state transitions (such as a change in viewership rights, or the birth of a new record in the system). Via smart contracts, we would log patient-provider relationships that associate a medical record with viewing permissions and data retrieval instructions (essentially data pointers) for execution on external databases. Included on the blockchain would be a cryptographic hash of the record to ensure against tampering, thus guaranteeing data integrity. Providers could add a new record associated with a particular patient, and patients could authorize sharing of records between providers. In both cases, the party receiving new information receives an automated notification to verify the proposed record before accepting or rejecting the data. This keeps participants informed and engaged in the evolution of their records.

The MVP prioritizes usability by also offering a designated contract which aggregates references to all of a user's patient-provider relationships, thus providing a single point of reference to check for any updates to medical history. In the MVP we handle identity confirmation via public key cryptography and employ a DNS-like implementation that maps an already existing and widely accepted form of ID (e.g. name, or social security number) to the person's Ethereum address. A syncing algorithm handles data exchange “off-chain” between a patient database and a provider database, after referencing the blockchain to confirm permissions via our database authentication server.

In the following sections we present the



[19] “Your medical record is worth more to hackers than your credit card” https://uk.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

[20] “Dark Web is fertile ground for stolen medical records” https://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html

design principles of our distributed system and its implementation.

Blockchain Background

Originally designed for keeping a financial ledger, the blockchain paradigm can be extended to provide a generalized framework for implementing decentralized compute resources. Each compute resource can be thought of as a singleton state-machine that can transition between states via cryptographically-secured transactions. When generating a new state-machine, the nodes encode logic which defines valid state transitions and upload it onto the blockchain. From there on, the blocks journal a series of valid transactions that, when incrementally executed with the state from the previous block, morph the state-machine into its current state. In a public chain the Proof of Work consensus algorithm and its underlying peer-to-peer protocol secure the state-machines' state and transitioning logic from tampering, and also share this information with all nodes participating in the system. Nodes can therefore query the state machines at any time and obtain a result which is accepted by the entire network with high certainty.

This transaction-based state-machine generalization of the blockchain is informally referred to as smart contracts. Ethereum is the first to attempt a full implementation of this idea. It builds into the blockchain a Turing-complete instruction set to allow smart-contract programming and a storage capability to accommodate on-chain state. We regard the flexibility of its programming language as an important property in the context of EHR management. This property can enable advanced functionality (multi-party arbitration, bidding, reputation, etc.) to be coded into our proposed system, adapting to comply with differences in regulation and changes in stakeholders needs.

The MVP utilizes smart contracts to create intelligent representations of existing medical records that are stored within individual nodes on the network. We construct the contracts to contain metadata about the record ownership, permissions and data integrity.

The blockchain transactions in our system carry cryptographically signed instructions to manage these properties. The contract's state transition functions carry out policies, enforcing data alternation only by legitimate transactions. Such policies can be designed to implement any set of rules which govern a particular medical record, as long as it can be represented computationally. For example, a policy may enforce that separate transactions representing consent are sent from both

patients and care providers, before granting viewing permissions to a third party.

To navigate the potentially large amount of record representations, our original MVP system structured them on the blockchain by implementing three types of contracts.

Smart Contract Structures

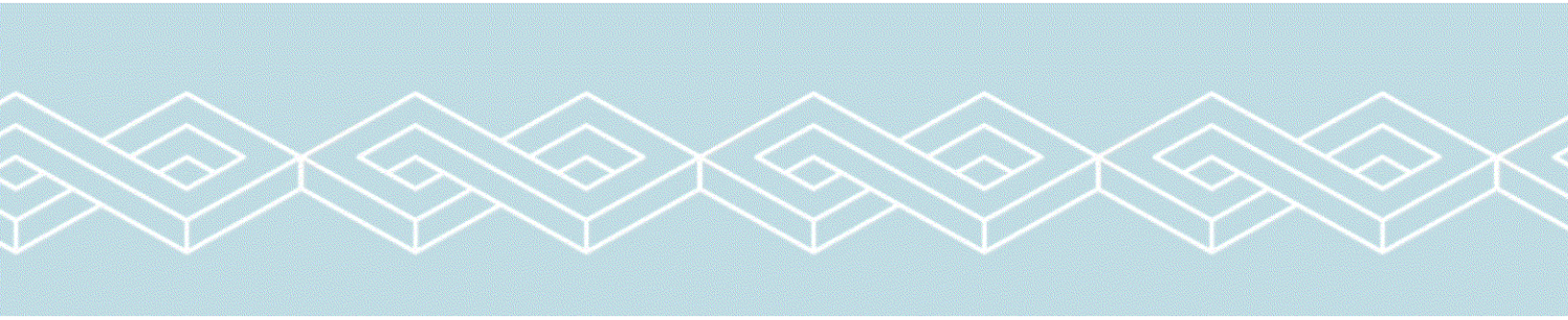
Registrar Contract (RC)

This global contract maps participant identification strings to their Ethereum address identity (equivalent to a public key). We intentionally use strings rather than the cryptographic public key identities directly, allowing the use of already existing form of ID. Policies coded into the contract can regulate registering new identities or changing the mapping of existing ones. Identity registration can thus be restricted only to certified institutions. The RC also maps identity strings to an address on the blockchain, where a special contract described below, called the Summary Contract, can be found.

Patient-Provider Relationship Contract (PPR)

A Patient-Provider Relationship Contract is issued between two nodes in the system when one node stores and manages medical records for the other. While we use the case of care provider and patient, this notion extends to any pairwise data stewardship interaction. The PPR defines an assortment of data pointers and associated access permissions that identify the records held by the care provider.
Each pointer consists of a query string that, when executed on the provider's database, returns a subset of patient data. The query string is affixed with the hash of this data subset, to guarantee that data have not been altered at the source. Additional information indicates where the provider's database can be accessed in the network, i.e. hostname and port in a standard network topology. The data queries and their associated information are crafted by the care provider and modified when new records are added. To enable patients to share records with others, a dictionary implementation (hash table) maps viewers' addresses to a list of additional query strings. Each string can specify a portion of the patient's data to which the third party viewer is allowed access.

Our prototype demonstrates this design with SQL data queries. In a simple case, the provider references the patient's data with a simple SELECT query conditioned on the patient's address. For patients, we designed a tool which allows them to



check off fields they wish to share through our graphical interface. Under the hood, our system formulates the appropriate SQL queries and uploads them to the PPR on the blockchain. Note that by using generic strings our design can robustly interface with any string queried database implementation. Hence, it can conveniently integrate with existing provider data storage infrastructure. At the same time, patients are enabled with fine-grained access control of their medical records, selecting essentially any portion of it they wish to share.

Summary Contract (SC)

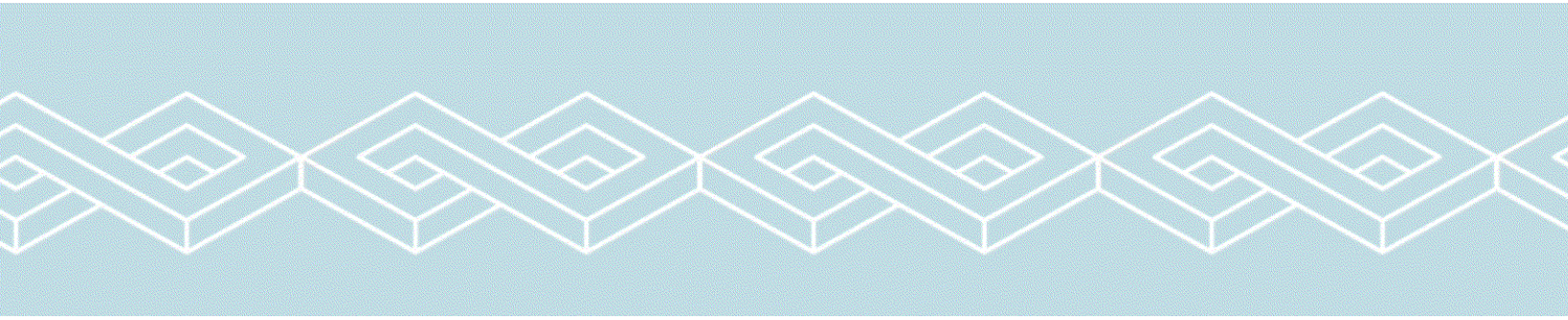
This contract functions as a bread crumb trail for participants in the system to locate their medical record history. It holds a list of references to Patient-Provider Relationship contracts (PPRs), representing all the participant's previous and current engagements with other nodes in the system. Patients, for instance, would have their SC populated with references to all care providers they have been engaged.

Providers, on the other hand, are likely to have references to patients they serve and third-parties with whom their patients have authorized data sharing. The SC persists in the distributed network, adding crucial backup and restore functionality. Patients can leave and rejoin the system multiple times, for arbitrary periods, and always regain access to their history by downloading the latest blockchain from the network. As long as there are nodes participating in the network, the blockchain log is maintained.

The SC also implements functionality to enable user notifications. Each relationship stores a status variable. This indicates whether the relationship is newly established, awaiting pending updates and has or has not acknowledged patient approval. Providers in our system set the relationship status in their patients' SC whenever they update records or as part of creating a new relationship. Accordingly, the patients can poll their SC and be notified whenever a new relationship is suggested or an update is available. Patients can accept, reject or delete relationships, deciding which records in their history they acknowledge.

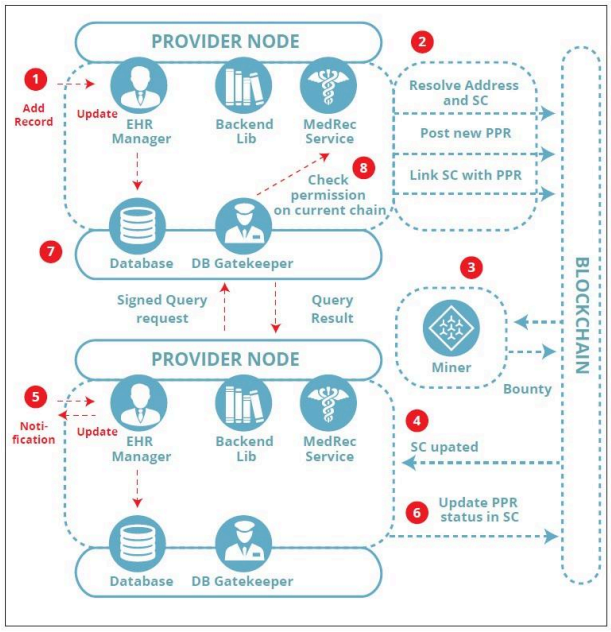
Our prototype ensures that accepting or rejecting relationships is done only by the patients. To avoid notification spamming from malicious participants, only providers can update the status variable.

These administration principles can be extended, adding additional verifications to confirm proper actor behavior.



System Node Description

We design the components of our system nodes to integrate with existing EHR infrastructure. We assume that many nodes, and in particular care providers, already trustfully manage databases with patient
data stored on servers with network connectivity. Our design introduces four software



components: Backend Library, Ethereum Client, Database Gatekeeper and
EHR Manager. These can be executed on servers, combining to create a coherent, distributed system. We provide a prototype implementation of these components that integrates with a SQLite database and is managed through our web user interface.

Notably, any provider backend and user interface implementations can participate in the system by employing the modular interoperability protocol as defined through our blockchain contracts. Patient nodes in our system contain the same basic components as providers. An implementation of these can be executed on a local PC or even a mobile phone. Their local database can be one of many lightweight database implementations. The databases can function merely as cache storage of the patient's medical data. Missing data can be retrieved from the network at any time by following the node's Summary Contract.

Primary Software Modules

Backend API Library

We construct multiple utilities, bundled in a backend library, to facilitate the system's operation. Our library abstracts the communications with the blockchain and exports a function-call API. Record management applications and their user interfaces can thus avoid the hurdles of working directly with the blockchain. One such hurdle is verifying that each sent transaction is accepted with high confidence by the network. Our library automatically handles the uncertainty of when transactions are mined and deals with cases when they are discarded. The backend library interacts with an Ethereum client to exercise the low-level formatting and parsing of the Ethereum protocol.

Steps 1 and 2 in Figure 2 illustrate our backend implementation of a scenario where a provider adds a record for a new patient. Using the Registrar Contract on the blockchain, the patient's identifying information is first resolved to their matching Ethereum address and the corresponding Summary Contract is located. Next, the provider uploads a new PPR to the blockchain, indicating their stewardship of the data owned by the patient's Ethereum address. The provider node then crafts a query to reference this data and updates the PPR accordingly. Finally, the node sends a transaction which links the new PPR to the patient's Summary Contract, allowing the patient node to later locate it on the blockchain.

Ethereum Client

In the original MVP this component implements the full functionality required to join and participate in the Ethereum blockchain network. This handles a broad set of tasks, such as connecting to the peer-to-peer network, encoding and sending transactions and keeping a verified local copy of the blockchain. For our prototype implementation we used PyEthereum and the PyEthApp client.

We modified the client to be aware of our mapping of identity and addresses. We then implement a service to locate the node's Summary Contract (SC), via Registrar Contract address lookup. This service runs continuously within the client to monitor real-time changes to the SC. In the event of an update, the service signals the EHR Manager to issue a user notification and, if necessary, sync the local database.

Steps 4 to 6 in Figure 2 continue the use case described above from the patient node perspective. The patient's modified Ethereum client continuously monitors her

SC. Once a new block is mined with the newly linked PPR, the client issues a signal which results in a user notification. The user can then acknowledge or decline her communication with the provider, updating the Summary Contract accordingly. If the communication is accepted, our prototype implementation automatically issues a query request to obtain the new medical data. It uses the information in the new PPR to locate the provider on the network and connect to its Database Gatekeeper server.

Database Gatekeeper

The Database Gatekeeper implements an off-chain, access interface to the node's local database, governed by permissions stored on the blockchain. The Gatekeeper runs a server listening to query requests from clients on the network. A request contains a query string, as well as a reference to the blockchain PPR that warrants permissions to run it. The request is cryptographically signed by the issuer, allowing the gatekeeper to confirm identities. Once the issuer's signature is certified, the gatekeeper checks the blockchain contracts to verify if the address issuing the request is allowed access to the query. If the address checks out, it runs the query on the node's local database and returns the result over to the client.

Steps 7 to 9 in Figure 2 illustrate how a patient retrieves personal data from the provider node.
Note that our components similarly support third-parties retrieving patient-shared data: the patient selects data to share and updates the corresponding PPR with the third-party address and query string. If necessary, the patient's node can resolve the third-party address using the Registrar Contract on the blockchain. Then, the patient node links their existing PPR with the care provider to the third-party's Summary Contract. The third party is automatically notified of new permissions, and can follow the link to discover all information needed for retrieval. The provider's Database Gatekeeper will permit access to such a request, corroborating that it was issued by the patient on the PPR they share.

EHR Manager

We tie together all the software components previously mentioned with our EHR management and user interface application. The application renders data from local databases (designed to be interchangeable with other DB software) for viewing, and presents the users with update notifications, and data sharing and retrieval options. Our user interface prioritizes intuitive, crisp, and informative design, as recommended by the

Department of Veteran Affairs and ONC's Blue Button design competition. The application is conveniently accessed through a web interface, built on a python backend framework. We are especially cognizant of compatibility for mobile devices, as modern users expect easy access and high quality experiences while on-the-go.

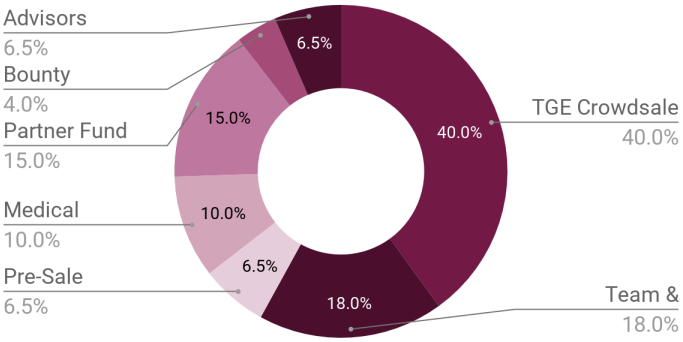
Authentication

A key factor is how we ensure that only the right people can get access to the right data. We achieve that by the rules database. Authentication to that is by password, token, or later, Smart Card with 1, 2 or 3 FA[21] to provide robust information about both patient and doctors identity.

Anticipated MediChain Network Development

1. Diagnostic Devices
2. Associated Algorithms
3. Personal Monitoring
4. Academic Medical Studies
5. Medical Insurers[22]
6. EMR Integration[23]
7. Telemedicine
8. National Resources

The MediChain Tokens made available for sale in connection with the a Token Generation Event ("TGE") will



Allocation

The Utility Tokens for MediChain (MCUs) made available for sale in connection with The Token Generation Event ("TGE") will be allocated as follows:

1. Pre-Sale Maximum 6.5%
2. Public Sale 40%
3. Partner Fund 15%
4. Team & founder Fund 18%
5. Advisors 6.5%
6. Medical Data Fund 10%
7. Bounty 4%

1 MCU has a nominal release value of $1 US. All unsold tokens will be burned.

[21] 1FA - tap or swipe the card
2FA Chip and pin or chip and password,
3FA Chip and pin plus fingerprint or iris scan.
[22] SmartCard Integration at this stage

[23] Electronic Medical Records

Pre-Sale 6,500,000 MCU

6.5% of MediChain tokens MCU will be distributed at presale. That will be five million sold and one point five million bonus tokens

Public Main Sale 40,000,000 MCU

40% of MediChain tokens MCU will be sold through the public sale. Received funds will be used toward the operations of the MediChain for the next five years. This includes development, administration, marketing, financial and legal consultancy, etc.

Use of public sale funds

The received funds will be allocated to initiatives concerning business development, multi-stakeholder model, as well as academic research, education, and market expansion.
A portion of funds will be used to facilitate building partnerships to promote the use (and therefore the value which increases according to number of users) of MediChains. This focuses on 'locked-in' growth of MediChain use with specific partners.
System Integration Funds are part of the partnership fund and will be used to facilitate the adoption of the MediChain in integrations of selected medical applications, including building markets where necessary. This focuses on growth through mainstream acceptance of MediChain.
Funds will be used to sponsor academic research, educational materials for developers, as well as promotion of MediChain technologies and contributions to open source communities. Some of the planned activities include:

- Establishing research labs in cooperation with high-profile universities;
- Creating tutorials and educational materials for MediChain developers;
- Cooperation with other open source communities;
- Events and conferences to raise the awareness of the MediChain technology and facilitate market adoption.

This focuses on credibility, profile and ability to respond to changes for MediChain.

Milestones for Internal Fund Release and Proportion of Funds Allocated

		2018	2019	2020+
M&BD		5%	5%	10%
Eng		10%	10%	2%
CLF		5%	5%	5%
RP:		15%	15%	10%

Key [costs including salaries, facilities and overheads]. :

M&BD: Marketing & Business Development
Eng: Engineering (Blockchain & Offchain); Security
CLF: Compliance, Legal & Financial
RP: Research Partners (funding)
The percentages in the green section are percentages of the presale. The percentages in the purple section are percentage of the TGE funds received. Gross spending is not expected to drop off, only the percentage attributable to the initial sale of MCU utility tokens.
RP is a major contributor to M&BD in the first three years as the company's reputation and profile will be spread by the doctors and scientists using the databases amongst potential data consuming clients. RP funding is typically in the form of three year program grants each to build a major data set, typically $250K-$1M USD.
Overheads including administration and premises are taken at 42%. It is expected that revenue will accrue after year 1 with break even in year 3. The expectation in the main model (although not the only possible source) is that this revenue will come from sales of anonymised big dara.

Medical Data Growth Fund 10.000,000 MCU

10% of tokens will be reserved for funding actions that add high-value medical data to the ecosystem through funding Research Grants and nonprofit academy research groups.

Partner Fund 15.000,000 MCU

15% of tokens will be reserved for future specialists and future rounds of investment, and distributed among future partners and subsidiaries created to promote data uptake.

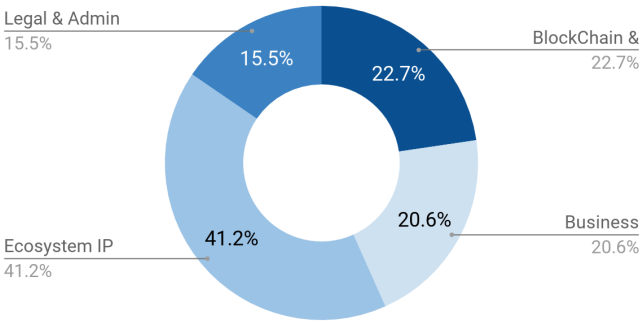
Team & founder Fund 18.000,000 MCU

18% of tokens will be reserved for future specialists and distributed among future partners, founders and team members, current and future, including future executive rewards.

Vesting

Three vesting schedules are used:
6000000 vest at 8% per month for early contributors

Funds raised by sale of MediCoin Tokens in the Token Generation Event ("TGE") are expected to be allocated as follows yrs 1-3



6000000 vest at 3% per month for lock in for long term employees.

6000000 vest after the ICO or at a point where all main sale tokens have been sold.

The focus here is ensuring the long term future of MediChain.

Advisors 6,500,000

Bounty 4,000,000

Allocation of Resources

100,000,000 MCUs will be issued. Nominal value $1 US

Use cases

The patient experience I

Demonstration of security of the blockchain

Alice, the patient, visits Dr **B**ob, the Medical services provider. She provides **B**ob with specific classes of data by accessing the blockchain with her MediChain Smart Card. Dr **B**ob's systems have unfortunately been compromised. Craig, the password cracker, has a keylogger on Dr **B**ob's computer, but is unable to get access to data from **A**lice's Smart Card as she is using a chip and pin card. Eve the eavesdropper is a passive attacker who has installed a keylogger and spyware that can see what Dr **B**ob can see, but cannot access **A**lice's access codes or any other part of **A**lice's data. Likewise **M**allory, the active attacker, tries to use man-in-the-middle attacks but without **A**lice and **B**ob's Smart Cards, she cannot get access to the actual blockchain. The integrity of the blockchain is preserved.

The patient experience II

Alice, the patient, visits Nurse Dan, a different Medical services provider. Nurse Dan performs specific medical tests on her (anything from blood tests to EEG to NMR and beyond) and adds the results of them

to her blockchain with his Smart Card, signing the addition and Alice's encrypting it. Later, on another day Alice provides Dr Bob with the results from Nurse Dan's tests by accessing the blockchain with her MediChain Smart Card.
Although her data may be compromised if Dr Bob has not cleaned up his computer, the integrity of the blockchain is preserved.
Over time Walter, one of the system wardens, detects patterns of misuse on Dr Bob's system and Craig, Eve and Mallory are identified and tracked down with varying degrees of difficulty.
Two years later Alice visits specialist Professor Francine who accesses all of Alice's data to make an algorithm-informed smart diagnosis based on longitudinal symptoms, treatments and responses.

The patient experience III

Alice, the patient, uses Faythe's trusted advisory service to find the best insurers for someone with her background by giving Faythe broad but anonymised access to Alice's blockchain without revealing personally identifiable details.

Medical Devices

Alice, the patient, uses wearable monitors like those in the Apple Healthkit ecosystem or Home health hubs to acquire her personal data and add it to her blockchain. These are available for future analysis by authorised apps & algorithms, doctors or specialists.

Algorithmic Analysis Services

Olivia manages Alice's blockchain and reading the rule network that Alice has allowed specific algorithms to access relevant parts of Alice's data. Alice is now alerted automatically when specific, harmful trends are found in her vital traces such as LVH indicators in her ECG picked up by her smart devices. In that case this reduces her risk of unexpected fatal cardiac events by approximately 50%

Medical Research

Olivia manages Alice's blockchain and reading the rule network that Alice has allowed specific types of researchers to access relevant parts of Alice's data. Professor Francine now has access to thousands of patient's data, fully anonymised, and in this case, voluntarily contributed by people like Alice through allowing limited access to their blockchains.

Insurers I

Again, Olivia manages Alice's blockchain and reading the rule network that Alice has allowed specific algorithms to access relevant parts of Alice's data. Alice has allowed that data to be accessed by her Medical Insurer. Alice is now called in for treatment when specific, harmful trends are found in her vital traces improving her quality of life and lifespan, decreasing premiums and increasing profitability for the insurer.

Insurers II

Una, the insurance data scientist, has been given access to a subset of the data that Professor Francine has, having to pay those patients who agreed to share data. Some have allowed messaging to their anonymised accounts, so Una knows that she has 52,342 anonymous addresses who she can offer a preferential policy to and can pay to campaign to them (or even target with display ads if they have opted into this), but will not know who any of them are unless they respond.

Locations

Impact Hub Kings Cross. 34B York Way, Kings Cross, London N1 9AB

China Hong Kong City,33 Canton Road, Tsimshatsui, Kowloon, Hong Kong

One Embarcadero Center, Suite# 500, San Francisco, California, 94111 (post token sale US office)

Team

Dr Mark Baker: CEO & Founder

Oxford Doctorate (D.Phil) Cancer Research, and Medical Research Council Fellow Brain and Behaviour Centre, Oxford University and the Radcliffe Infirmary, NHS Oxford, Cambridge Research Fellow Neuroscience, former CTO at Peerius, Europe's Largest User of Secured, Privacy Enhanced Big Data for Predictive Analytics, Data Specialist at Janssen Pharmaceutical, Developer's of security solutions used by Governments against Hackers, C & Python developer.

Dr Nicolas Roydon Smoll: Medical Doctor, Epidemiologist/Big Data Analyst

Medicine/Surgery, Monash University. Researcher at the School of Population and Global Health at the University of Melbourne, in Melbourne, Australia.

Ron Cafferky: Electronic Health Records Specialist

Experienced Clinical Informatics Manager with a demonstrated history of working in the hospital & healthcare industry. Skilled in managing clinical reporting issues on varied platforms. Thrives when working with data and solving challenging database issues.

Samuel Dare: Blockchain Engineer

Experienced Blockchain technologist: Bit Core, Ethereum, Corda, Hyperledger, BigChainDB, Solidity, Smart Contracts. Past clients have included Governmental bodies and the International Development.
Has a development background developing in Python (5 years), Javascript (5 years), NodeJS (3 years), Go/Golan (1 year) Solutions Architect roles.

Agustin Cassani: Blockchain Engineer

More than 10 years of web and mobile development in a wide range of technologies, most of them related to JavaScript such as Node.js, Express, Koa, React, Redux, Flux, AngularJS, Angular, React Native, Ionic, Ionic 2, and NativeScript.

David Forbes: Software Developer

Keen problem solver with experience in both Frontend and Backend development using C++, Java, C#, PHP, SQL, JavaScript, CSS, HTML and Drupal. Has worked in a variety of industries with past clients including government agencies and Real Estate within Australia.

Katy Blackwell: Operations Chief

Highly experienced attorney and operation consultant assisting businesses regarding regulatory & HR compliance, process improvements, intellectual property, mediation and contract negotiations.

Giannis Stathopoulos: Business Development & Digital Marketing

Highly experienced operations and growth manager specialized in startups. Digital, blockchain enthusiast and entrepreneur.

Mark Shorter: Creative Director/UX Specialist

20+ years of experience designing for digital media with a proven knowledge of creative strategy, vision and leadership to every situation. Committed to creating enjoyable, useful, and engaging experiences regardless of medium. Passionate about building design teams that function well together and are inspired to create great work.

Naomi Ellis: Public Relations, Marketing & Design

Experienced writer, multidisciplinary designer and creative thinker. Excellent communicator. Experience in the tech industry as a Marketing and Community Lead. Startup business growth hacker. Skilled in Content Creation and Art Direction.

Fred Fooks: Business Development

Meng graduate from Engineering Science at Oxford University. Previous experience in an investment firm that specialises in technology start-ups. Contributed specifically to the growth plans of three start-ups.

Technology:

Rob Moya: UX/UI Designer

Rob is an expert on front-end development and providing a great UI/UX design. Mr. Moya has 7+ years of experience on user interface design and front end development experience for startups and small companies in the US and China. Product launches, MVPs, Landing pages, React web apps, WordPress sites, with more than +100.000 active users per month.

Business Development:

Yilin (Linda) Wen: Business Development

Experienced Business Development Analyst and Consultant

Matt Ganeles: Business Development

Over 2 years of experience in project management, data management and customer support. Over 1 year of digital marketing experience, specific to ICOs and cryptocurrency. Participated in the planning, execution, and support stages of a successful $10.8 million ICO. Passionate about new alt-coins and crypto markets.

Advisors:

Simon Cocking: Blockchain Advisor

Senior Editor at Irish Tech News, Editor in Chief at CryptoCoinNews, and freelances for Sunday Business Post, Irish Times, Southern Star, IBM, G+D, and other publications. Top ranked member of the 'People of Blockchain' (most recently ranked at 1/1000). Business mentor and advisor working with 20+ successful ICOs to date. Named on 10 global Twitter influencer lists in the last 12 months. Speaker at TEDx, Web Summit, Dublin Tech Summit, and overseas in Dubai, Singapore, Moscow, Tel Aviv, Madrid, Tbilisi, Riga, Porto, Dublin and Helsinki in the last 12 months. He has been based in Ireland for over 22 years and has co-founded or founded six successful companies.
#4 in top 1000 global list for People of Blockchain
#10 in world's most influential fintech voices on Twitter

Jon Matonis: Cryptocurrency Specialist

Jon Matonis is a Founding Director of the Bitcoin Foundation and his career has included senior influential posts at VISA International, VeriSign, Sumitomo Bank, and Hushmail.
An economist and e-Money researcher focused on expanding the circulation of nonpolitical digital currencies, Jon also serves as an independent board director to companies in the Bitcoin, the Blockchain, mobile payments, and gaming sectors. Jon has been a featured guest on CNN, CNBC, Bloomberg, NPR, Al Jazeera, RT, Virgin Radio, and numerous podcasts. As a prominent fintech columnist with Forbes Magazine, American Banker, and CoinDesk, he recently joined the editorial board for the cryptocurrency journal Ledger. His

early work on digital cash systems and financial cryptography has been published by Dow Jones and the London School of Economics.

Mike Raitsyn

Serial entrepreneur and early stage investor, specializes in fintech, internet marketing and process automation. Cofounder in more than 12 successful companies. Founder of ICOBox.
More than 30 ICOs and $300m+ raised.

Keith Teare

A leading figure past and present in many important companies including Accelerated Digital Ventures, Archimedes Labs, Minds and Machines Inc, MedCo, EasyNet and RealNames to name just a small few, Keith is a founding shareholder of Techcrunch.

Gabriel Zank

Fintech entrepreneur-Advisor. Founder of MobileyourLife and involved in the AI-Fintech space providing solutions in the B2B space. ICO advisory in Fundraising Capital and International Business Development

Chris Fennell: US Legal & Legal Compliance

Partner at Wilson Sonsini Goodrich & Rosati. Law practice focuses on corporate and securities law, including general corporate representation, seed and venture capital financings, public offerings and mergers and acquisitions.

Amarpreet Singh: Blockchain Engineer

Technology/Digital enthusiast and a seasoned professional with years of experience in Tech industry – operations, consulting and innovation. His professional background includes working with tier 1 firms such as Microsoft (APOC Operation Manager), the World Bank (Senior Infrastructure Consultant and Economic Advisor), Airbus etc., and advising startups and speaking at various technology forums. His educational background includes B.E. (Computer Science) and three Masters degrees from three Universities around the globe (including MBA from National University of Singapore). Due to above mentioned professional and educational background, Amarpreet has lived/worked/studied in India, Singapore, France, China, South Africa, Korea etc., and traveled to many more countries for work.

Simon Choi: International Legal Compliance

Simon Choi is an international lawyer, qualified to practise law in England & Wales, and in Hong Kong, China. Simon graduated from the law schools' of Peking University, the University of London and the University of Hong Kong respectively. Simon has advised more than 10 ICO projects globally and contributes to MediChain.io by providing an in-depth knowledge of international law, as well as advising and reviewing new blockchain regulations in various jurisdictions. With more than 25 years of experience in international trade, investment, finance, and M&A, he is an asset for MediChain.io ensuring the highest degree of compliance and adherence to all relevant government policies towards blockchain technology.

Summary

MediChain uses blockchain technology to create a distributed ledger of medical information on a per patient basis with a separate distributed ledger index. To establish trust and usability we will test and establish using data from the UK which will still have a global marketable value to researchers and pharmaceutical companies.
Personal data is secured within the blockchain by three levels of security. MediChain data is secured initially through device tokens and user passwords but is designed to rapidly use Smartcards with 2FA similar to chip and pin banking.

Acknowledgements

1. http://ieeexplore.ieee.org/abstract/document/7573685/
2. Tsung-Ting Kuo Hyeon-Eui Kim Lucila Ohno-Machado *Blockchain distributed ledger technologies for biomedical and health care applications*
   Journal of the American Medical Informatics Association, Volume 24, Issue 6, 1 November 2017, Pages 1211–1220, https://doi.org/10.1093/jamia/ocx068
3. "Who Owns Medical Records: 50 State Comparison." Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. Aug. 20, 2015. [Online] Available: http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison

4. U.S. Department of Health and Human Services, Office of Civil Rights. (2013). 45 CFR Parts 160, 162, and 164. “HIPAA Administrative Simplification.” [Online] Available: http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf
5. Mandl, Kenneth D., David Markwell, Rhona MacDonald, Peter Szolovits, and Isaac S. Kohane. “Public Standards and Patients' Control: how to keep electronic medical records accessible but private.” Bmj 322, no. 7281 (2001): 283-287.
6. Office of the National Coordinator for Health Information Technology. (2015). Report to Congress. “Report on Health Information Blocking.” [Online] Available: https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf
7. “Individuals’ Right Under HIPAA to Access their Health Information 45 CFR § 164.524." U.S. Department of Health and Human Services. [Online] Available: http://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/access/. Accessed: Aug. 8, 2016.
8. Grossmann, Claudia, W. Alexander Goolsby, LeighAnn Olsen, and J. Michael McGinnis. Institute of Medicine of the National Academies. “Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good.” Workshop Summary (Learning Health System Series). National Academies Press, (2010).
9. Kish, Leonard J., and Eric J. Topol. "Unpatients [mdash] why patients should own their medical data." Nature biotechnology 33, no. 9 (2015): 921-924.
10. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
11. Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In Security and Privacy Workshops (SPW), (2015) IEEE, pp. 180-184.
12. Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum Project Yellow Paper (2014).
13. “The Patient Record: health design challenge.” The Office of the National Coordinator for Health Information Technology, U.S. Department of Veterans Affairs. Jan. 2013. [Online] Available: http://healthdesignchallenge.com/

Risk Factors

The purchase of MCU tokens involves a high degree of risk, including but not limited to the risks described below. Before acquiring MCU tokens, it is recommended that each participant carefully weighs all the information and risks detailed in this Whitepaper, as well as the information and risks available from other sources.

(a) Dependence on Computer Infrastructure. MCU tokens and MediChain dependence on functioning software applications, computer hardware and the Internet, implies that MediChain can offer no assurances that a system failure would not adversely affect the use of MCU tokens. Despite MediChain's implementation of all reasonable network security measures, its processing center servers are vulnerable to computer viruses, physical or electronic break-ins or other disruptions of a similar nature. Computer viruses, break-ins or other disruptions caused by third parties may result in interruption, delay or suspension of services, which would limit the use of the MCU tokens.

(b) Smart Contract Limitations. Smart contract technology is still in its early stages of development, and its application is of experimental nature. This may carry significant operational, technological, regulatory, reputational and financial risks. Consequently, although the audit conducted by independent third party increases the level of security, reliability, and accuracy, this audit cannot serve as any form of warranty, including any expressed or implied warranty that the MediChain smart contract is fit for purpose or that it contains no flaws, vulnerabilities or issues which could cause technical problems or the complete loss of MCU tokens.

(c) Regulatory Risks. Blockchain technology, including but not limited to the issue of tokens, may be a new concept in some jurisdictions, which may then apply existing laws or introduce new regulations regarding blockchain technology-based applications, and such regulations may conflict with the current MediChain smart contract setup and MCU tokens concept. This may result in the need to make substantial modifications to the MediChain smart contract, including but not limited to its termination, the loss of MCU tokens, and the suspension or termination of all MCU tokens functions.

(d) Taxes. MCU tokens holders are solely responsible for determining if the transactions contemplated herein are subject to any applicable taxes whether in their home country or in another jurisdiction. It will be the sole responsibility of MCU tokens holders to comply with the tax laws of any

jurisdictions applicable to them and pay all relevant taxes.

(e) Force Majeure. MediChain's performance may be interrupted, suspended or delayed due to force majeure circumstances. For the purposes of this Whitepaper, force majeure shall mean extraordinary events and circumstances which could not be prevented by MediChain and shall include: acts of nature, wars, armed conflicts, mass civil disorders, industrial actions, epidemics, lockouts, slowdowns, prolonged shortage or other failures of energy supplies or communication service, acts of municipal, state or federal governmental agencies, other circumstances beyond MediChain's control, which were not in existence at the time of Whitepaper release.

(f) Disclosure of Information. Personal information received from MCU tokens holders, the information about the number of tokens owned, the wallet addresses used, and any other relevant information may be disclosed to law enforcement, government officials, and other third parties when MediChain is required to disclose such information by law, subpoena, or court order. MediChain shall at no time be held responsible for such information disclosure.

(g) Value of MCU tokens. Once purchased, the value of MCU tokens may significantly fluctuate due to various reasons. MediChain does not guarantee any specific value of the MCU tokens over any specific period of time. MediChain shall not be held responsible for any change in the value of MCU tokens.

(h) Risk of Insufficient information. MCU tokens are at a very early developmental stage and its philosophy, consensus mechanism, algorithm, code and other technical specifications and parameters could be updated and changed frequently and constantly. While the Whitepaper contains the up-to-date key information related to MCU tokens at the date of the Whitepaper, it is not complete nor is final and is subject to adjustments and updates that MediChain may make from time to time. MediChain is not in a position, nor obliged to report on every detail of the development of MCU tokens and other elements of the system presented by MediChain and therefore will not necessarily provide timely or full access to all the information relating to the MCU tokens, but will use reasonable efforts.

Legal Disclaimer

PLEASE REVIEW CAREFULLY THE PRESENT SECTION "DISCLAIMER OF LIABILITY". IF YOU HAVE ANY DOUBTS AS TO WHAT ACTIONS YOU SHOULD TAKE, WE RECOMMEND THAT YOU CONSULT WITH YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S). No part of this Whitepaper is to be reproduced, distributed or disseminated without including this section "Disclaimer of Liability".

The information set out below may not be exhaustive and doesn't imply any elements of a contractual relationship or obligations. The sole purpose of this Whitepaper is to present MediChain and MCU tokens to potential token holders in connection with the proposed token sale. Despite the fact that we make every effort to ensure the accuracy, up to date and relevance of any material in this Whitepaper, this document and materials contained herein are not professional advice and in no way constitutes the provision of professional advice of any kind. To the maximum extent permitted by any applicable laws, regulations and rules, MediChain doesn't guarantee and doesn't accept legal responsibility of any nature, for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising from or related to the accuracy, reliability, relevance or completeness of any material contained in this Whitepaper. Further, MediChain does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity, person, or authority, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this Whitepaper. You should contact relevant independent professional advisors before relying or making any commitments or transactions based on the material published in this Whitepaper.

This Whitepaper is not subject to any legal system and is not governed by any law. No regulatory authority has examined or approved of any of the information set out in this Whitepaper, and no such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this Whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

You don't have the right and shouldn't buy MCU tokens if you are a citizen or resident (tax or otherwise) of any country or territory where transactions with digital tokens and/or digital currencies are prohibited or in any other manner restricted by applicable laws. Purchased MCU tokens cannot be offered or distributed as well as cannot be resold or otherwise alienated by their holders to mentioned persons. It is your sole responsibility to establish, by consulting (if necessary) your legal, tax, accounting or other professional advisors, what limitations, if any, apply to your particular jurisdiction and situation, and ensure that you have observed and complied with all such restrictions, at your own expense and without liability to MediChain.

MCU tokens are not and will not be intended to constitute securities, digital currency, commodity, or any other kind of financial instrument and have not been registered under relevant securities regulations, including the securities laws of any jurisdiction in which a potential token holder is a resident. This Whitepaper is not a prospectus or a proposal, and its

purpose is not to serve as a securities offer or request for investments in the form of securities in any jurisdiction. However, in spite of the above, legislation of certain jurisdictions may, now or in future, recognize MCU tokens as securities. MediChain does not accept any liability for such recognition and/or any legal and other consequences of such recognition for potential owners of MCU tokens, nor provide any opinions or advice regarding the acquisition, sale or other operations with MCU tokens, and the fact of the provision of this Whitepaper doesn't form the basis or should not be relied upon in matters related to the conclusion of contracts or acceptance investment decisions. This Whitepaper doesn't oblige anyone to enter into any contract, to take legal obligations with respect to the sale or purchase of MCU tokens, and to accept any crypto currency or other form of payment. Potential owners of MCU tokens are advised to contact relevant independent professional advisors, on the above matters.

Certain statements, estimates and financial information contained herein constitute forward-looking statements or information. Such forward-looking statements or information involve known and unknown risks and uncertainties, which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements. Further, all examples of calculation of income and profits used in this paper were provided only for demonstration purposes or for demonstrating the industry's averages. For avoidance of doubt, nothing contained in this Whitepaper is or may be relied upon as a guarantee, promise, representation or undertaking as to the future performance of MediChain and/or MCU token, and/or promise or guarantee of future profit resulting from purchase of MCU token.

MCU tokens cannot be used for any purposes other than as provided in this Whitepaper, including but not limited to, any investment, speculative or other financial purposes. MCU tokens confer no other rights in any form, including but not limited to any ownership, distribution (including, but not limited to, profit), redemption, liquidation, property (including all forms of intellectual property), or other financial or legal rights, other than those specifically set forth below. While the community's opinion and feedback can be taken into account, MCU tokens do not give any right to participate in decision-making or any direction of business related to the MediChain service.

Section that immediately follows this disclaimer, is written solely for the good faith purpose of saving your time, and in no case should be understood as recommendation not to read the whole Whitepaper.

English language of this Whitepaper is the primary official source of information about the MCU tokens, any information contained herein may from time to time be translated into other languages or used in the course of written or oral communications with customers, contractors, partners etc. In the course of such translation or communication some of the information contained herein may be lost, corrupted or misrepresented. In the event of any conflicts or inconsistencies between such translations and communications and this English language of Whitepaper, the provision of this English language of Whitepaper as original document shall prevail.