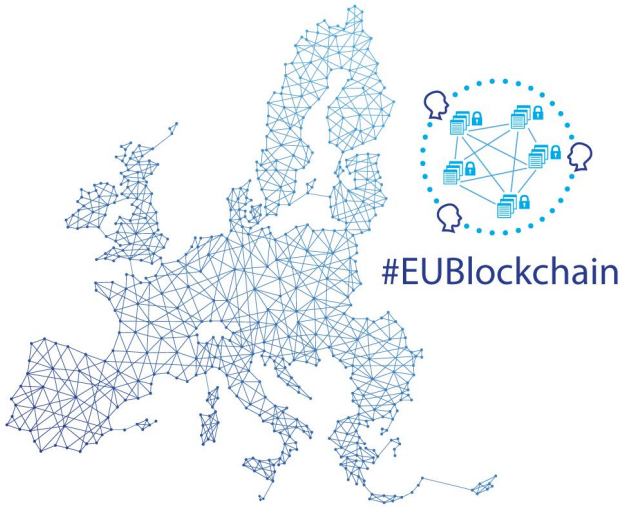
EU Blockchain Observatory and Forum

An initiative of the European Commission

EU BLOCKCHAIN OBSERVATORY & FORUM

Workshop Report - Use cases in healthcare – Frankfurt, 4 September, 2019



By the European Commission, Directorate-General of Communications Networks, Content & Technology.

Author: Tom Lyons
Published on Oct 14, 2019
Comments and inquiries may be addressed to the following email: info@eublockchainforum.eu

Table of Contents

Introduction to the day

Blockchain: EU strategy and key initiatives

Chiara Mazzone and Pierre Marro (European Commission, DG CNECT)

- The EU is taking a holistic approach to blockchain with the goal of establishing the region as a global leader in blockchain and DLT
- Measures include
    - The European Blockchain Partnership (EBP) and the development of the European Blockchain Services Infrastructure (EBSI)
    - A public-private partnership in the form of the International Association of Trusted Blockchain Partnerships (INATBA)
    - Connecting global and European expertise under the aegis of the European Union Blockchain Observatory and Forum
    - Investing in EU research, innovation and startups the the Connecting Europe Facility and H2020 programmes as well as the new EU investment scheme for AI and blockchain (including a support program)
    - Promoting and enabling a Digital Single Market (DSM) legal framework, interoperable standards and skills development
    - Organising a major conference, Convergence - The Global Blockchain Congress - in Málaga between 11-13 November (www.blockchainconvergence.com)

Current and future perspectives on eHealth policies & blockchain

Reza Razavi, PhD, European Commission DG CONNECT – Communications Networks, Content and Technology; Directorate H – Digital Society, Trust and Cybersecurity; Unit H3 – eHealth, Well-being & Ageing

- The EU is in the process of transforming healthcare in Europe in order to improve services for citizens, empower citizens when using digital health services, facilitate person-centred care, give citizens better access to their health data everywhere in the EU and connect share health data for research, faster diagnosis and better health outcomes.
- Data-driven healthcare is the motto. Every family doctor should eventually have access to superior digital services at his or her desk, including artificial intelligence and supercomputing.
- The “Data Package” of 25 April contained five components for a common data space in the EU for new products and service based on data
    - Communication on Digital Health and Care
    - Communication on Artificial Intelligence

    - Communication on sharing of Private Sector data
    - Review of the Directive on the re-use of Public Sector Information (PSI)
    - Results of the evaluation of the Database Directive
- There are specific strategies for AI, which is central to personalised medicine. As put forth in the Communication Artificial Intelligence for Europe (COM(2018) 137 final, these include:
    - Increasing investment
    - Strengthening R&I
    - Making more data available
    - Empowering users
    - Nurturing talent in the space
- Supercomputing will be another key element to success in this realm. The EuroHPC (High Performance Computing) joint declaration to participate in the European and national effort to build and deploy a world-class computing and data infrastructure in Europe. Overall ca. 1 billion euros will be invested by 2020 with the goal of ranking among the world's top three infrastructures by 2022-2023.
- As noted, the EC is also highly supportive of blockchain technology.
- Under the H2020 eHealth cybersecurity research and innovation effort, there was a call for proposals in 2018 for improving cybersecurity in hospitals. While the call did not mention blockchain, among the 40 submitted proposals, 15 had blockchain in them, and among the 7 selected for funding, 5 contained a blockchain component. These were:
    - FeatureCloud
    - Serums
    - Sphinx
    - Panacea
    - Curex
- There are a number of eHealth funding opportunities available 2021-27
    - Digital Europe Programme and Connecting Europe Facility
    - Horizon Europe
    - European Social Fund and European Globalisation Adjustment Fund European Regional Development Fund
    - InvestEU Programme
- Under the Digital Europe Programme, the Commission has suggested a 9.2 billion euro total investment investment, many areas of which touch on eHealth. The overall investment aims are:
    - Digital transformation and interoperability (1.3 billion)
    - High performance computing (2.7 billion)
    - Artificial intelligence (2.5 billion)
    - Cybersecurity and trust (2 billion)
    - Advanced digital skills (0.7 billion)

Presentation – The State of Blockchain in Healthcare and Life Sciences

Heather Leigh Flannery, Global Lead, ConsenSys Health; Chair, P2418.6 Blockchain in Healthcare Standards Development Working Group, IEEE SA; Co-Founder & Chair, Blockchain in Healthcare Global ("BiHG"), IEEE ISTO; Co-Chair, HIMSS Blockchain Task Force; Chair, Enterprise Ethereum Alliance (EEA) Healthcare Special Interest Group (SIG)

- We should not think of blockchain in isolation but rather in the context of a number of rapidly maturing technology innovations that affect healthcare (AI, 3D printing, Biotech/Genomics, Internet of Medical Things (IoMT)). The present moment is as if the Gutenberg press, the steam engine and the integrated circuit had all been invented at the same time. The results will be revolutionary and unpredictable.
- At the same time we as a society have reached a moral and cultural tipping point regarding the just use of personal data (and there is no data more personal than health data). Business models based on the monetising of anonymised or pseudonymised patient data without remuneration to the original data subject are rapidly ending. Patient self-sovereignty is on the rise.
- In addition to data monetisation there has also historically been a lack of data access; today data subjects have the least access to their data. That is changing, among other things thanks to:
    - The GDPR in Europe
    - United States 21st Century Cures Act, which defines "data blocking" as an illegal action. This will prevent healthcare organisations form keeping data from data subjects.
- Among the priorities that underpin the use cases we need to focus on are:
    - **Privacy-in-Depth.** We need to find ways to allow the use of medical data for the greater good in privacy-preserving ways. For example, for AI training the thinking used to be that you need to move data to the algorithm to train it. Now we can do machine learning with techniques that allows the algorithm to go to the data and learn. This is more secure and privacy-preserving. Among the techniques relevant to privacy-in-depth are:
        - **Bioethics.** We have not had a bioethics upgrade since the 1970s. The time has come. Many open questions. For instance: what is health data? If my self-driving car is monitoring my heart rate, is that medical data?
    - **Cybersecurity.** Healthcare data have only been the targets of cybercriminals for the last 10 years or so, so the industry is not yet hardened to that. At the same time we have accelerating amounts of health data being generated and new devices coming online at a rapid pace. That makes for massive vulnerabilities and increasing attacks. The industry needs to respond.

    - **Compliance.** As platforms and services become increasingly cross-border and pan-jurisdictional, the ability to be able to mandate or enforce compliance in an automated way is required. Right now it is very hard to audit. There is a huge burden on regulators and the regulated. Building that capability into the next generation of technology is important.
- When we talk about blockchain, we are talking about more than just the technology. The broader discussion includes:
    - Decentralised Apps (dApps) and the new Web 3 user experience
    - Various types of blockchain networks, including public, private and hybrid networks
    - Tokenised assets
    - Smart contracts which can provide secure automation across organisational boundaries
    - Privacy-in-depth, which includes
        - Zero-Knowledge Proofs (ZKPs)
        - Trusted Execution Environments (TEEs)
        - Secure Encrypted Virtualization (SEV)
        - Blind Computation
        - Verifiable Computation – Hardware and Algos
        - Secure Multi-Party Computation
        - Differential Privacy
        - Homomorphic Encryption
        - Quantum-Resistant Encryption
    - Decentralised AI, including:
        - Federated learning in blockchain networks
        - Intelligent agent-based automation
        - Optimization w/agent-based simulation
        - New paradigm in training data provenance
- Today is the first time we have the chance, thanks to blockchain technology and cryptoeconomics, to apply behavioral economics and game theory to make things work better. Can we alter incentives to create new business models and encourage convergent innovations?
- Identity will be key for these kinds of innovation in healthcare and life sciences. There is work to extend existing self-sovereign identity standards, like those from the Decentralised Identity Foundation, to healthcare needs. For example, extending the DID and DIF standards with health-specific metadata.
- Networks of non-fungible tokens (NFTs) could be used to compartmentalise data; replacing one massive identity with compartmentalised data and so prevent the dangers of cross-referencing.
- Doing this will require among other things a framework for multiple biometric attestations: what levels or assurance are necessary, what biometrics apply? This need not be binary. You can instead rely on degrees of assurance based on use case. Yet currently there is no standardised scale for such degrees of assurance.

- You cannot create digital identities, compartmentalised or otherwise, that cannot be recovered if needed (patient unconscious, keys lost). Recovery is part of the bioethical posture: recovery, reuse, grievances, etc.
- There are a number of use cases/approaches involving tokenisation and blockchain that could optimise the “bench to bedside” process. For example, multi-use self sovereign data and zero-knowledge proofs to provide alternatives to anonymised data brokerage markets; accelerating e-consent for inclusion of data in studies; etc.
- There are a number of promising initiatives already underway:
    - **Consortia:** EU IMI-Pharma Consortium; Synaptic Health Alliance; Health Utility Network; Coalesce Health Alliance
    - **US Government Professional Associations:** First ATO in US Federal Government (2018); US Centers for Disease Control carrying out multiple pilots; HIMSS Blockchain Task Force with more than 80 active members; Blockchian in Healthcare Global (BiHG) IEEE ISTO non-profit; IEEE SA P2418.6 Standards Development Working Group
    - **Representative Platform-Based Groups:** Enterprise Ethereum Alliance - Healthcare Working Group; Hyperledger Healthcare Working Group; Corda Healthcare Community teamed with HSBlox
- Promising use cases for blockchain in healthcare include:
    - Identity, Credentialing, Biometrics, Privacy, and Security
    - Patient Empowerment, Data Sovereignty, and Consents
    - Supply Chain from Manufacturing to Point of Care
    - NCD / Chronic Disease Prevention and Treatment, Enabling Care Coordination
    - Opioid Use Disorder Prevention and Treatment
    - Precision Medicine: Genomics, Wearables, IoMT, AI
    - Reg-tech, Clinical Trials
    - Post-Market Surveillance to Digital Therapeutics
    - Value-Based Care and Reimbursement; Real World Evidence
    - Mitigating Waste, Fraud, and Abuse
    - Mitigating Health Disparities, Embedded Ethics

Panel discussion – Blockchain in Clinical Trials

- *Dr. Olaf Wilhelm (Therawis Pharma/diagnostics)*
- *Dr. Axel Schumacher (Project Shivom)*
- *Moderated by Heather Flannery (ConsenSys, Observatory)*

- *Q: let us try and define the problem space, what is broken in research in clinical trials today?*

    - M: coming from pharma, clinical trials are an expensive and time consuming part of the value chain. Lots of stakeholders that don't trust each other or know each other. We need to implement certain controls along the process to establish trust. This is why clinical trials would be good for blockchain.
    - A: Data silos is a huge problem. People have difficulty accessing data sets, also with GDPR, they can't access and move data easily. But this can be solved. The first step is to empower patients, the second step is to break down the silos.
    - O: Developing a new drug has a 1 in 1000 chance of being successful, and to get all the way there costs on average 1 billion euros. A lot of parties and stakeholders involved. They don't trust each other. Another problem is that there are a lot of intermediaries. Also heavy compliance burden: we have to prove that the data produced during the trial are correct.
- *Q: For trials, how can we improve selection and recruitment? Many sites that get chosen to conduct trials struggle to recruit a single person.*
    - M: It is difficult for pharma companies to get the right sites for a clinical trials. Looking for patients with the right profile, etc. would be helped by an integrated database that is secure, transparent and integral and overarching (right now very centralised and dependent on the sites). More data convergence allowing stakeholders tp access and derive insights from larger data sets would be desirable. It is not necessary to do this on a blockchain, but blockchain can be a very good tool in terms of ensuring data integrity and transparency.
    - A: We would like a global database, if possible. Traditionally you have a problem that patients in clinical trials are from certain groups (most clinical trials are carried on white people).We need a global database of trial sites and phenotypes. So you can search for specific metadata. But it has to be of high quality. These things can be implemented using blockchain technology.
    - O: Today if a company wants to run a trial it sends the COO out to 100s of centers to interview physicians and nurses on how many suitable patients they have. It can take 6 months until you have a picture, but you still don't know if the data is good or how many other trials any particular center is doing at one time. That is also because the data is siloed. In Germany, cancer centers have to store data electronically. Germany has 15 such centers and each has its own system. It would be great to have a snapshot of how many centers, how many patients, and how many trials are happening at any one moment. Federated learning, where data stays at its point of origin, could be helpful. You can improve the efficiency of choosing centers.
- *Q: Are there better ways to design trials? Can we use these technologies to support remote clinical trials, and move to near real time, continuously available trial data analytics? Can blockchain help validating data from the Internet of Medical Things (IoMT) so that we can create patient self-reported data that is as clinically valid as any other?*

    - M: We are not quite there yet, but there is a move to drive clinical trials from traditional settings to more remote ones. Blockchain has no part here yet. But when you get to fully remote clinical trials blockchain becomes interesting.
    - A: Standards are important, as is working together. Different pharma companies should sit together if they want a solution. What is clear is that we will move pretty fast to technical solutions that can collect all this data, from medical devices, wearables, self-reported data, data that we will bring into connection with a person's genetic data for a net result. Then AI algorithms can crunch this data. But it is complex.The keyword here is interoperability, putting it together.
    - O: Another promising area is re-use of data. Imagine a company that has a new drug and ran 200 trials while developing it. What if you could get that data and simply re-use it for another study (assuming the data was immutable). This could lead to massive efficiencies. It might also have value in terms of patient safety because you may be able to see for instance what kind of patient should not get a certain drug.
- *Q: What parts of the process could be made "pre-competitive". Where does it make sense to foster cooperation before competition starts?*
    - A: This is a very important point: We need to create competitive consortia and encourage people to do this for data collection. But that is expensive. When it comes to collecting genetic data for clinical trials it makes sense that pharma companies join efforts. You have to sequence a person only once. But then you need strict control over how that data is handled, how it is shared. You can make rules for that with smart contracts. This too can increase efficiency and potentially save billions.
    - O: We already left competition behind a long time ago. The big guys have done this already. If you share information you also get information back. As long as it is embedded in the system who owns what, it works.
    - A: It is instructive to watch how money actually moves globally in this space. Many predict that in 4-5 years the biggest pharma company in the world won't be Novartis but Facebook, Amazon or TenCent. Data is that valuable.
    - O: Yes. Who owns the data will be the owner of the value. Ideally, it would be patients who own the data and the value!

QnA

- *They say that blockchain is disruptive. But today we have been talking about blockchain in the old, top-down paradigm: what the EC can do with it. What can we say in terms of bottom-up? Can we imagine a world in which perhaps 10 people across the world discover they have a rare disease and they band together to ask the pharma company to make them a drug?*
    - A: There is no way around empowering patients as well as, we shouldn't forget, healthy people. We want a system where no one gets sick. It is a learning curve. We need to educate citizens about their rights and also about the value of their

data. When it comes to consent and empowerment, how much do patients really understand what they are consenting to. Education is important. We need the tools to make it as easy as possible for lay people to understand what their data entails and how to make their data actionable.

Presentation – Convergence of Blockchain and Secure Computing for Healthcare solutions

Jonathan Passerat-Palmbach, PhD (ConsenSys, Imperial College)

- Markets for personal health data handled in privacy-preserving ways are one of the most important and promising use cases for blockchain at the moment.
- In future, we will be able to construct markets in which patients who go to a hospital can themselves keep the health-related data about them that is generated during their visit. Then we can provide the patient the option to share that data if he or she wants, and include options to share only under certain circumstances or only certain parts of that data. It would be akin to putting little padlocks on the different databases associated with the patient.
- The sharing would happen in a privacy-preserving way, so the patient's personal information would be protected. But since the data is also valuable, the patient could have options to monetise it and so an incentive to share. A data scientist training an AI could be interested for instance in this data to better his or her algorithm, and be willing to pay. And the data scientist would also be injecting value into the system with a better trained algorithm that could also be monetised. This could revolutionise how we pay for healthcare, for instance by creating decentralised marketplaces that create a win-win for all involved.
- This can be accomplished with the convergence of a number of emerging technologies, including: blockchain, artificial intelligence (including machine learning, deep learning, natural language processing and robotic process automation), Internet of Medical Things (IoMT), and advances in genomics and biotech.
- There are however major challenges too, including a) controlling access to data, b) storing and processing sensitive data, c) incentivising users to take part?, and d) preventing information leakage.
- Secure computation is the discipling of running applications on data that remain encrypted in one way or another. Today when data is processed, encryption can be used only to a certain point. To use the data, at some it must be revealed. And if data is revealed once, it is (potentially) revealed forever, even under the best circumstances. There are different approaches to secure computation. Four of the most promising, from the (currently) least to the most practical, are:

- **Homomorphic encryption:** the holy grail of secure computation, the idea is to allow computation on encrypted data, by finding a function that generates an encrypted result which would be the same as the result of the operations as if they had been performed on the unencrypted data.
- **Secure Multiparty computation:** the idea of splitting up computational tasks among multiple actors so that no one party has access to all the data.
- **Trusted Execution Environments (TEEs):** Secure processing on the micro-processor itself. Allows for the safe un-encryption of data, the performance of functions on it, and safe re-encryption.
- **Federated Computing/Learning:** The ability of a model to learn from data in a privacy-preserving way. This already is geing employed. For example, Google's predictive typing model learns from each user's behavior by being sent to the user's phone (the data never leaves the phone, only the learning). Blockchains can be used to orchestrate and provide an audit trail of the interactions between users and those using the data.

Panel discussion – Patient-Mediated Data Exchange, Aggregation, Curation, and Monetization

Participants

- *Jonathan Passerat-Palmbach, PhD (ConsenSys, Imperial College)*
- *Alexis Normand (Embleema)*
- *Dr. Eberhard Scheuer (HIT Foundation)*
- *Mirko De Maldè (My Health My Data, Lynkeus)*

- *Q: What is the single biggest barrier in the way of healthcare data exchanges today?*
  - User experience. We have to make cryptography and recovery simple for everyone. Even for computer scientists things can still be challenging to use.
  - Availability of data, which relies on interoperability. The US has done a great job of making data available, there are standards for patients so they can access and download their own data. That is a necessary first step: to exchange data you first have to have it.
  - The fact that, while everybody loves blockchain, they are afraid of crypto. Sometimes you have to reframe the message: from making cryptocurrency for health data exchange to instead building the infrastructure for it.
  - Motivation and incentive. Hospitals need some incentive to make data available. there are security issues plus they have to justify the time, effort and cost.
- *Q: What are the benefits and incentives for individuals, patients or otherwise, to aggregate data?*

    - An incentive doesn't have to be bound to financial rewards, and aggregation doesn't have to be bound to physical locations. For "well" (non-sick) patients the incentive can be improving their own health care, they might be interested in some process that could improve diagnoses in future, perhaps through AI. This may particularly be the case if an individual knows that he or she is susceptible to a certain disease, even if not yet suffering from it. So the incentive could be a way to improve one's own healthcare.
    - There are definitely benefits to aggregating data. Having one's full medical history can help with diagnoses. Today we have our health histories scattered all over the place. And it can be more than just reconciling data at a patient level. if you add your private lifestyle data to it, you can make patients accountable for what they are supposed to do for their care. If you can aggregate data at a systemic level you can better predict who is at risk.
    - We need data from all the different silos in order to do good research and develop good drugs. The only person who can aggregate patient data today in the Western world is the patient him or herself. The only way to change the behavior is to pay the people. So compensation as incentive.
    - The ability to have your data in one place is a big deal. You don't have that at the moment. This is something that would save a lot of time, cost, etc.
    - Incentives for healthy people are very different than for those who are sick. If you suffer from a rare disease you won't say no to it, because it is in your interest potentially in helping contribute to your own cure.
    - Another component is if the legal framework in place in order to aggregate data. Perhaps your data is not only you. If you share your genetic data that is not only about you but also your parents and ancestors.
- *Q: How can we handle curation of health data. The data should not be modifiable by the patient (or anyone else). Yet the patient is also the person most likely to identify errors in their data. So in some cases data needs to be modifiable. How could that work?*
    - AI is a good option in this respect. It can help you in identifying outliers in quality control assessments, help /flag data as 'not good enough'.
    - Only certain types of data are considered to be medically relevant. Not all patient-reported data is believable to a doctor anyway. With a blockchain you create traceability. It is the 'birth certificate for the data'. So you know where the data came from and when it was 'born.'
    - The immutability aspect is important. However, what is clinically relevant is also the patient-reported outcome. Patient has to monitor side effects, etc. So blockchain can help here as a proof of provenance and truth of the data.
    - Immutability is good as long as the data is good going in. Mistaken data is common. So it is important to have the process of data collection as automated as possible. Blockchain can help here both on the patient and clinic side.
    - Yet then we also have an issue of IoT security: how can we know the sensors are doing the right thing?

- *Q: If we have exchange, curation and aggregation, we can re-use data in many different contexts. What are the implications of such health data reuse?*
    - This isn't about input privacy but rather output privacy. You have to think in terms of a 'spending budget' on the privacy of the data you are giving out. The more you query this data, for example with an AI that trains on it, eventually you will remove the protection around it. So we have to know when data is spent to the point that it starts to reveal too much about the person.
    - All of this is possible only if you have consent. Here there is different feedback between the US and Europe. In Europe all are equal in terms of healthcare, it is seen as a basic right. As a result, monetising data is frowned upon. In the US it is seen quite differently: you can monetise data and bring down your copays. In Europe you could potentially have the patient freely give his or her monetisation to some patient's group.
    - The aspect of consent is very important in this context. Once data is digital it is so easy to copy and reuse. It is fair if someone donates data for research to compensate them. We already do this for taking part in clinical trials.
    - Dynamic consent is interesting here. We can attach consent to a piece of data along with the conditions under which it is given. That can then go out, so researchers see those conditions.
- *Q: In monetisation scenarios, there is a question of discovering the value. So you need a market, either explicit or implied. What it going to take to get us there, or should not go there?*
    - It is a culture thing. You can think of monetisation as a way to compensate people, but also as a way to relieve the burden on the health service. There will be a time when we will be faced with pragmatic questions like can we still afford to run public health like we do now. If the answer is no then maybe monetisation is a way to generate value.
    - It costs between 200 and 20,000 dollars to recruit for a clinical trial. The average value of healthcare data per person is more like 20 dollars. The market will depend on the rarity of the disease or the data.
    - In terms of consent, no matter where the data is, I would always want to first be asked if it is ok to use my data. And then they would have to make an offer. You can use the blockchain as a message board - people can post for the kind of patients they are looking for, and make an offer.
    - With My Health My Data, a new project for an individual data exchange in Europe, the problem is how to understand how to make a commercial offer for data without direct monetisation, and to come up with an economic model that makes sense.
    - Health relevant data is a broad field, it is not just clinically relevant data. If I lose weight on a diet incentive program, that is health relevant too. If I have been vaccinated that is health relevant.
    - If there were open marketplaces for data, data could be priced differently in different parts of the world. If this was available on the blockchain, for

researchers it would be good to know in what markets data originate. There are good byproducts from data markets besides just the financial incentives.

Appendix

Workshop slides

- Workshop - Use cases in Healthcare - Overview Slides
- Blockchain: EU strategy and key initiatives
- Current and future perspectives on eHealth policies & blockchain
- The State of Blockchain in Healthcare and Life Sciences
- Convergence of Blockchain and Secure Computing for Healthcare solutions

Workshop videos

- Videos from this and all other workshops can be found on the EU Observatory website under reports.
- Videos specific to this workshop:
    - Healthcare workshop Part 1
    - Healthcare workshop Part 2
    - Healthcare workshop Part 3
    - Healthcare workshop Part 4
    - Healthcare workshop Part 5

Official agenda

Time	Activity
9:15	**Registration**
10:00	**Introduction of the day - Agenda and objectives of the day**
10:05	**Presentation and introductory words from the European Commission** Chiara Mazzone, Pierre Marro (European Commission, DG CNECT) Reza Razavi (European Commission, DG CNECT)
10:30	**Presentation – State of Blockchain and Healthcare** Heather Flannery (ConsenSys, Observatory)
11:10	**Panel discussion – Blockchain in Clinical Trials** Dr. Olaf Wilhelm (Therawis Pharma/diagnostics); Dr. Axel Schumacher (Project Shivom); Moderated by Heather Flannery (ConsenSys, Observatory)
12:15	**Presentation – The use of cryptographic tools and convergence of blockchain with other technologies for healthcare solutions**

	Jonathan Passerat-Palmbach, PhD (ConsenSys, Imperial College)
13:00-14:10 Lunch break	
14:10	**Panel discussion – Patient-Mediated Data Exchange, Aggregation, Curation, and Monetization** Dr. Eberhard Scheuer (HIT Foundation); Mirko De Maldè (My Health My Data, Lynkeus); Jonathan Passerat-Palmbach, PhD (ConsenSys, Imperial College); Alexis Normand (Embleema); Moderated by Heather Flannery (ConsenSys, Observatory)
15:10	**Working Sessions – Opportunities for Clinical Trials, Health Data Exchange, and Supply Chain** All participants
16:15	**Conclusion**
16:30	**End of the day**