Securing Transparency and Governance of Organ Supply Chain Through Blockchain

Nicanor Chavez[1], Stefan Kendzierskyj[1], Hamid Jahankhani[1], Amin Hosseinian-Far[2]
[1] Northumbria University, London UK; [2] Northampton University, UK,

Abstract: The governance and supply chain of organs is a complicated process throughout the life cycle; from the outset of pre-assessment of organ placement, it's supply chain journey and important post donor analysis. Healthcare organisations face a huge challenge in the diverse collation of data that are held in systems which are mostly in silo operation and little scope for interoperability or accessibility of medical data. Lack of data access or trust in its accuracy makes the task more challenging and problematic for healthcare institutions whose preference undoubtedly would be to focus their energies on the decision-making side of a patient's health in assessing organ donor suitability and urgency to organ match due to the receiving patient criticalities, rather than time and resources spent on validating data authenticity, etc. There are further complications that can occur in potential mix-ups of organs, contamination of DNA during organ transplant, non-ethical organ supply and audit trail transparency related to these activities. There is a serious question on how to create a single source of the truth and blockchain may provide the best possibilities. Blockchain is becoming a more sought-after technology being used in the healthcare space due to its attributes of immutability, traceability and security whilst providing that assurance of transparency and audit trail. Blockchain looks to be a good fit to manage the supply chain of organ procurement/placement and an audit control method to analyse data in any pre or post operation event. Combined with the right processes, in the form of a cyber security framework/maturity model for the healthcare industry, would ensure that all those who signed

up to the blockchain deployed for the supply chain logistics would respect the ethics and requirements and expect transparency for those authorised to access. However, some challenges exist in GDPR compliancy of data that would exist on a certain proposed blockchain models and needs further exploring with regards to benefits in data held off-chain.
Keywords: Blockchain, Supply Chain, GDPR, Organ Trafficking, Transplant Tourism

1. Organ Supply Chain Through Blockchain

Organ transplant is a critical area of healthcare as those patients in need will have an urgency and priority that puts additional pressure across all those involved in the touch points of organ supply chain. The following data underlines this pressurised situation. According to the UK National Health Service (NHS) Blood and Transplant most current online information (circa April 2019), there have been 1,735 people who have received an organ transplant and 6,282 people who are still waiting to get a transplant in the UK. This equates to the unfortunate result of people dying daily while they wait for the correct match. In its 2018 reports, The Global Observatory on Donation and Transplantation (part of the World Health Organization, WHO) reported a total of 44,219 organs transplanted within the European Union; while the European Commission (in its European Organs Directive) reported that during 2017, there was a total of 34,000 organ transplants while 60,000 patients were on waiting lists in 800 different organ transplant programmes. The organ transplantation cycle is composed of several types by activities that involve the donation and extraction of human organs, most commonly being the kidneys, liver, lungs and heart that get transplanted (NHS Blood and Transplant, April 2019). During all phases of this cycle, a big amount of data related to donors, organs and patients gets recorded in different computer systems and printed in multiple ways to provide health organizations and physicians the information needed to take proper decisions on organ allocation and medical procedures, which then is read, analysed and moved around in hardcopy format that could potentially be lost, copied or printed with typographical errors, thus potentially leading to erroneous decisions or violating medical and data regulations.

The difficulty is further heightened with the challenge of system accessibility and interoperability of medical records and other data sets, due to the disparate and diverse type systems and infrastructure. Typically, it is not just the disparate infrastructure but types of structured/unstructured data and its applications and how to access all in a single source of the truth. There is an enormous volume of data held amongst hospitals, clinics, pharmacies and labs that also makes difficult to authenticate, track its journey and audit. Since data is a key element but there is also supply chain physical components (the organs) then there needs to be a mechanism that can ensure all data is captured, interoperable, cannot be tampered, etc.

To improve efficiency and transparency it is suggested in this chapter to propose the use of blockchain and smart contracts as a way of governing the organ donor matching and transplantation. Also, to help organise the pre/post-surgery medical activities by trying to identify whether there could be a mix-up of organs or contamination of DNA during the organ transplant cycle that could affect the proposed system, as well as activities related to DNA sampling and recording in a public blockchain. Finally, data protection and ethics that are inherent to supply chain governance where activities and practices related to public health are involved. To support ethics and governance it is beneficial to operate a cyber security maturity model (CSMM) alongside blockchain requirements. That means all organisations that require to be part of organ supply chain run on blockchain architecture must comply with the supply chain prerequisites and a maturity model can effectively monitor all through control methods, training and other that help keep a high discipline and compliance. It is then easier to warn those that consistently fail to comply, are below standard and deploy methods to change the behaviour. Through blockchain all information related to a patient's health as well as to the entire organ donation and transplant related activities (analysing potential organ donors, donor-recipient matching, laboratory tests, transplantation, pre/post operation and DNA sampling) can be tracked. The data will come from multiple systems and record specific non-patient identifiable information in the blockchain.

Blockchain technology offers great potential in the healthcare industry; it is estimated that 55% of healthcare applications will have adopted blockchain for commercial deployment by 2025 (Statista, 2019), while at the same time the healthcare sector suffers the highest toll of system data breaches with 2.5 times the

global average when comparing to other industries, being about $380 per single patient record compromised in 2017 (Forbes, 2018).

One key concern in healthcare is the management of sensitive information, its data sharing and security due to the application of the General Data Protection Regulation (GDPR) in the UK and the European Union. Blockchain can help to avoid sensitive data retention by enabling the 'disclosing without exposing' of data, with the use of its cryptographic techniques and methods.

2. Organ Trafficking and Transplant Tourism

Compounding the structural issues of data interoperability, transparency and so on is the darker side of organ supply where the urgency to source organs creates and stimulates a demand where criminals often interact and thrive in. The WHO reports this international trade on the rise where those vulnerable may sell their kidney for $1000 (WHO, 2004). This crosses ethics where criminals contaminate supply chain with 'non-ethical' sourced organs (those that sell organs and illegally traffic) and transfers across a number of third parties where organisations who require to be bona fide and ethical can end up procuring trafficked organs. The US Department of State (2019) quotes how a lot of criminal activity is mapped in and around human trafficking and as mentioned often affecting the most vulnerable in society.

Organ trafficking, and transplant tourism takes place when a person who needs the transplant travels to a different country to purchase the required organ, often from a donor who is in financial need (Budiani-Saberi & Delmonico, 2008). Organ commercialism is on the rise and several business models and job roles have been created as of result of this (Jafar, 2009). Jafar (2009) refers to such business models and job roles as 'profitable enterprises' and goes on to argue that such activities exploit poor donors in an illegal and unregulated form. In 2008 at the Istanbul Summit, a declaration was signed by participating members, with a view to promote regulation of organ procurement, and assert that physicians and regulatory bodies of the donor's and recipient's counties should prohibit transplant tourism (Steering Committee of the Istanbul Summit, 2008; Abboud et al., 2008). This summit symbolised one of the key collective international efforts to curb the unethical practices involved in organ trafficking and exploitation of the vulnerable and the poor. Soon after the declaration of Istanbul Summit, and in response to that,

the Canadian Society of Transplantation and the Canadian Society of Nephrology introduced a similar policy document to inform Canadian healthcare stakeholders when conducting transplant healthcare (Gill et al, 2010). In a more recent study, Ambagtsheer et al. (2013) conducted a qualitative study on kidney procurement and organ trafficking in Netherlands and affirms that identifying such unethical trades is a challenging task, due to poor reporting, and the complexities involved. Bagheri & Delmonico (2013) anticipated that the key solution to the problem would be an international agreement that is formal, biding that imposes legal liability. There are already some existing regional and international rules and policy guidelines related to organ, tissue and cell trafficking (Council of Europe., 1997; Caplan et al., 2009), however, Pietrobon (2016) argues that implementing such conventions is not a straightforward task, due to the transnational nature of the convention implementation, and low willingness shown by some of the participating countries and authorities. One of the solutions to overcome this would be to enhance cross-border collaboration, information sharing, joint prosecution efforts, and transnational law enforcement structures (Holmes et al., 2016). Abmagtsheer (2019) assessed two case studies of Trafficking in Human Beings for the purpose of Organ Removal (THBOR) where both cases were investigated by police and they went through prosecution. He concluded that in both cases, the complexities, the number of stakeholders and other relevant obstacles have made the process extremely challenging. Furthermore, the lack of awareness by different stakeholders contributes to the poor implementation of such transnational efforts (Holmes et al., 2016). Abmagtsheer (2019) argues that investigation and prosecution should not be deemed as the only key approach in tackling THBOR, and therefore, efficient legal organ supply and procurement, and processes for victims' protection should be enhanced, irrespective of the processes involved for investigation and prosecution. Another perspective to this is the role that physicians and healthcare providers play. Caulfield et al. (2016) believe that health care professionals and physicians can enact a significant role in curtailing organ trafficking. Patients (the donor, the recipient, or both) discuss the available options in the first instance with the medical professionals. The second phase of communication occurs when they provide their medical solution choice related to the transplantation, and the final interaction phase, referred to as 'post-transplantation' phase, is when the operation has been completed. Therefore,

physicians and medical professional can potentially curtail the illegal organ trade throughout all the above three phases (Caulfield et al., 2016). Considering the existing information, it is apparent that there is little or no comprehensive research work on the adoption of suitable technologies to monitor and regulate organ procurement and operation, and more importantly to restrain illegal activities within the context.

Crucially, it is why a blockchain mechanism could potentially solve many issues of authenticity, tracking and for those institutions in the supply chain that need that security there but a transparency to be able to view data where permissioned.

3. Blockchain and Healthcare Operability

Blockchain is a decentralised network of different peers interconnected as an open distributed ledger (or database) which can efficiently record transactions in a permanent and verifiable manner. Bitcoin is today perhaps the most widely used P2P (peer to peer) digital currency which was first released in a white paper at the end of 2008 by the pseudonym of Satoshi Nakamoto (Nakamoto, 2008). Bitcoin's enormous success triggered a massive surge of 'crypto currencies' where hundreds of alternative currencies were created and traded, making a total market cap of $215.00B traded in October 2019 (Coincap, 2019). Although having its roots in cryptocurrency, blockchain technology, besides from offering decentralization, offers industry real tangible benefits in the form of a high level of transparency, immutability and security via algorithmic consensus mechanisms. One of the key features of blockchain and particularly important for this study is that it provides a mechanism of unfalsifiable time-stamping transactions (smart contracts) which stores and tracks them in a secure and verifiable way, enabling the share of the information in real time. This is extremely useful for patients and healthcare organizations as this helps them to control their records and provides a higher level of transparency and security to all participants within the blockchain and instilling a sense of authenticity when analysing multiple data sets. A key benefit to blockchain technology is that every user can maintain their own copy of the ledger" (Yaga et al, 2018). This is an important statement regarding one of the basic features of a blockchain, because when there is a central repository of data, a user needs to trust that the administrator keeps regular and proper backup of the system, as centrally

managed databases might be lost, destroyed or corrupted. Moreover, whenever a new user (or node) joins a blockchain network, it 'scans' or looks for other nodes and gets a full copy of the blockchain ledger, making it very difficult for the ledger to be destroyed or lost, and being in a P2P configuration, the blockchain is resilient to the loss of individual or multiple nodes.

Blockchain is already implemented for healthcare organizations, and Agbo et al, (2019) make the case for the increased privacy and security in the access of data through the use of cryptographic algorithms that encrypt data stored in blockchain, ensuring that only the users who get access permissions are able to decrypt it; moreover since the patient identity gets pseudonymized by the use of cryptographic keys, their data can be shared by all stakeholders without revealing the identity of the patient in question and therefore cam respect certain privacy aspects.

There are various types of blockchains depending on the data that will be managed, its availability and the type of actions that participants will be able to perform in the system. The following table details the comparison between these types of architectures:

	Permissionless Public	**Permissionless Private**	**Permissioned Public**	**Permissioned Private**
Participation	Anyone can join and act as a node	Anyone in the private network act as a node	Only nodes in a predetermined criterion can act as a node	Only chosen nodes in a private network can act as a node
Security	Very High	Low	Medium	Low
Speed	Very Low	Fast	Slow	Very Fast
Trust Level	Mistrusted	Trusted	Mistrusted	Trusted

Table 1- Comparison among blockchain architectures

As mentioned, one of the benefits of blockchain is that it removes the need of a central authority that enables the system to administer transactions; this allows participants in the blockchain to perform transactions in a distributed environment and eliminates the problem of a single point of failure improving their speed without being affected by the delay that a central authority adds. Instead blockchain uses a consensus mechanism which determines the conditions that need to be met for the nodes within a system whether to accept to add a block in the blockchain, this way

reconciling discrepancies and agreeing the transaction is valid or not. There are numerous types of consensus algorithms. Some of the most relevant/popular below are discussed by Fernandez and Fraga while reviewing the use of blockchain for the Internet of Things (Fernandez, Fraga, 2018):

- **Proof of Work (PoW):** used in Bitcoin, it requires the miners to solve complex problems to get the right to verify new transaction.
- **Proof of Stake (PoS):** requires less computational power than PoW, consuming less energy.
- **Practical Byzantine Fault Tolerant (PBFT):** this solves the Byzantine Generals Problem for asynchronous environments. PBFT assumes that less than a third of the nodes are malicious. For every block to be added to the chain, a leader is selected to be in charge of ordering the transaction. Such a selection has to be supported by at least 2/3 of the all nodes, which have to be known by the network.
- **Delegated Proof-of-Stake (DPoS):** is similar to PoS, but stakeholders instead of being the ones generating and validating blocks, they select certain delegates to do it. Since less nodes are involved in block validation, transactions are performed faster than with other schemes.
- **Delegated BFT (DBFT):** is a variant of BFT where, in a similar way to DPoS, some specific nodes are voted to be the ones generating and validating blocks.
- **Ripple consensus algorithm** was proposed to reduce the high latencies found in many blockchains, which are in part due to the use of synchronous communications among the nodes. Thus, each node relies on a trusted subset of nodes when determining consensus, what clearly reduces latency.
- **Stellar Consensus Protocol (SCP):** is an implementation of a consensus method called Federated Byzantine Agreement (FBA). It is similar to PBFT but, whilst in PBFT every node queries all the other nodes and waits for the majority to agree, in SCP the nodes only wait for a subset of the participants that they consider important.
- **Sieve:** is a consensus algorithm proposed by IBM Research that has already been implemented for Hyperledger-Fabric. Its objective is to run non-

deterministic smart contracts on a permissioned blockchain that makes use of BFT replication.

The healthcare organisation would need review its objectives, network and way of working in order to select the blockchain model and consensus algorithm. The following Table2 shows a summary comparison between the different types of blockchain and consensus algorithms (101Blockchains, 2019):

Consensus Algorithms	Blockchain Platform	Launched Since	Programming Languages	Smart Contracts	Pros	Cons
PoW	Bitcoin	2009	C++	No	Less opportunity for 51% attack Better Security	Greater energy consumption Centralization of Miners
PoS	NXT	2013	Java	Yes	Energy efficient More decentralized	Nothing-at-stake problem
DPoS	Lisk	2016	JavaScript	No	Energy efficient Scalable Increased security	Partially centralized Double spend attack
LPoS	Waves	2016	Scala	Yes	Fair usage Lease Coins	Decentralization Issue
PoET	Hyperledger Sawtooth	2018	Python, JavaScript, Go, C++, Java, and Rust	Yes	Cheap participation	Need for specialized hardware Not good for Public Blockchain
PBFT	Hyperledger Fabric	2015	JavaScript, Python, Java REST and Go	Yes	No Need for Confirmation Reduction in Energy	Communication Gap Sybil Attack
SBFT	Chain	2014	Java, Node, and Ruby	No	Good Security Signature Validation	Not for Public Blockchain
DBFT	NEO	2016	C++, C, Go, Kotlin, JavaScript	Yes	Scalable Fast	Conflictions in the Chain
DAG	IOTA	2015	Javascript, Rust, Java Go, and C++	In Process	Low cost network Scalability	Implementation gaps Not suited for smart contracts
POA	Decred	2016	Go	Yes	Reduces the probability of the 51% attack Equal contribution	Greater energy consumption Double signing
PoI	NEM	2015	Java, C++XEM	Yes	Vesting Transaction partnership	Decentralization Issue
PoC	Burstcoin	2014	Java	Yes	Cheap Efficient Distributed	Favoring bigger fishes Decentralization issue
PoB	Slimcoin	2014	Python, C++, Shell, JavaScript	No	Preservation of the network	Not for short term investors Wasting coins
PoWeight	Filecoin	2017	SNARK/STARK	Yes	Scalable Customizable	Issue with Incentivization

Table 2 - Comparison among consensus mechanisms

3.1. Blockchain Governance

A common misconception regarding blockchain networks is that they run wild without ownership or control. This is not particularly true as permissionless blockchain networks are governed often by software developers who have a large degree of influence on where blockchain should deploy. The users can reject any change from the developers by declining to install any updates, or publishing nodes which have some degree of control as they create and publish any new block; they all play an important role in the blockchain governance, even when there is not a central authority. Permissioned blockchain networks rely on a governance structure that controls access and enforces rules, responding to incident including cyber threats - because of the degree of trusts among the participants, this type of network commonly uses less computationally intensive consensus mechanisms (English et al, 2018).

There are two areas that must be considered when creating a blockchain system:

- Blockchain Governance - which refers to the processes and structure that determine how the blockchain will be maintained and will evolve over time.
- Solution Governance - this refers to the set of rules that will regulate how different groups or organizations will interact with each other.

Complementing the points mentioned above, The IBM Corporation in their paper 'The Founder's Handbook" (IBM, 2018) includes six governance elements to consider when working in the governance strategy for a blockchain:

1. **Data**: questions like who will own the data, what will be the data-related security need of the network? A defined security strategy along a distinct ownership of data must be in place before the blockchain is deployed into production.
2. **Marketplace**: this element is aimed for blockchains which are created to generate revenue, so the main question will be what will be the model in place, how this revenue will be shared and if the participants of the network will get incentives to join if they will be allowed to generate income-related applications over the blockchain.
3. **Participation**: this covers all actions related to network access and enrolment (on boarding / off boarding) of participants, and what will happen to data when a participant leaves the blockchain.

4. **Technology**: this must be covered during the early stages of the blockchain creation, as questions on infrastructure costs, coding related, level of privacy required, and other tech strategies must be thought with the aim to support the solution as it continues to grow.
5. **Transactions**: as different types of solutions that will run on the blockchain are evaluated, questions related to the number of participants and the types of transactions must be discussed and answered.
6. **Smart Contracts**: a very key and important aspect, as a blockchain depends on smart contracts, which help to establish trust within the network via the rules that help to govern them.

It will be important for any organization to follow tested cybersecurity standards and their guidelines in order to assure the security of all systems that interact with/ or that the blockchain network will use. These standards will provide a strong base to protect a blockchain network from attacks, for example: any organization who aims to build a blockchain network, must ensure that all networks, systems and computer equipment used is patched and accesses are properly administered following best practices in order to avoid compromising it due to security breaches. This is where the concept of adhering to a cyber security maturity model can be of effective potential to the whole supply chain and provide a methodology to benchmark for a high level of compliance and security.

4. The Organ Transplantation Life Cycle

The lifecycle of organ transplantation is not a straightforward process. On the one side is the complex and ethical approach to define the matching and delicate management of this and all its associated data. On the other side is the physical element to supply chain of the organ and the convoluted process of packaging, storage and transportation often against a time driven requirement (Venanzi et al., 2013). Supply chain needs to ensure time is keep to a minimum as ‘time the organ is without vascularization’.

To help define a human organ, tissue and cell donation can come from three sources: Living, Non-living and Cadaveric. Within the living donor type, there are the ‘living related donors’ (a blood related of the potential recipient of the organ), the ‘living un-related donors’ (not a blood related but with emotional ties to the

recipient), and there can be also a third type which is the ‘altruistic donor’ who volunteer to donate an organ (most commonly a kidney) without previous knowledge of the recipient. Sometimes there is an ‘offer’ from a brain-dead patient, and the hospital needs an agreement from the relatives in order to approve the donation of the organ.

In a formal hospital environment, only these types of living donors are allowed to become part of the organ donation cycle in Europe and in the United States of America, otherwise they are blocked as this could potentially be a case of organ trafficking.

Health organizations and hospitals must have a well-established organ allocation system with at least one list of patients waiting for a transplant. Regarding the ‘waiting list’, the recipient patient gets evaluated along with the donor that potentially will provide the organ with a series of medical tests performed to both on them, and all the information recorded allows the system to perform some complex calculations to reveal whether the donor and the recipient are a match and the organ can be offered.

4.1. Donor Matching and pre-surgery related activities

The detection of potential donors is probably the most difficult activity to be subject of very rigorous standards and protocols. There are three tests that are performed to evaluate donors:

- **Histocompatibility** (or blood matching): determines if the donor’s blood is compatible with the recipient.
- **Crossmatch**: The cross-matching test is very important part of the living donor medical examination analysis and is repeated again just before the transplant surgery: the blood from the donor and the recipient are mixed, and if the recipient’s cells attack and kill the donor cells, then the crossmatch is considered positive meaning that the recipient’s has antibodies against the donor cells (and therefore they are incompatible); if the crossmatch is negative, then both donor and recipient are ‘compatible’.
- **HLA testing**: The HLA test or ‘leukocyte antigen’ is a quite complex blood test that involves antigens which are proteins (or markers) inside the cells of the body that distinguish each individual as unique. For organ transplantation, there are six antigens markers that have shown to be most

important; both donor and recipient receive an HLA testing in order to determine their level of compatibility of these markers according to a score.

When a donor and a recipient's HLA markers are the same (or at least very close to each other's percentages), then it is determined that they are compatible and the organ then can be used for people (recipients) that are part of the 'waiting list': the very first person with negative crossmatch and closes percentage HLA marker matching from this list takes the organ.

	HLA type recipient				HLA type donor	
Patient	A	A	B	B	Acceptable HLA-A antigens	Acceptable HLA-B antigens
1	A2	A29	B7	B44	A 69, 68, 74, 31, 32, 33	B 55, 56, 70, 72, 42, 45, 50, 54, 61, 71, 75, 13, 41, 48, 49, 59, 62, 76, 77, 18, 35, 38, 47, 60, 67,* 39,* 64,* 8,* 65*
2	A29	A68	B14		A 69, 33, 34	B 39, 65, 67, 55, 71
3	A2	A11	B7	B51	A 69, 68, 3, 32,* 74,* 25,* 34,* 66*	B 55, 78, 35, 53, 56, 71, 52, 54, 70, 72, 75, 76, 77, 18, 42, 58, 81, 59,* 64,* 65,* 67,* 38,* 39*
4	A*0101	A*0201	B*0702		A 36, 69, 68, 74*	B 55, 42, 81, 67*
5	A24		B7	B62	A 23	B 76, 55, 70, 72, 75, 77, 56, 71, 42, 46, 54, 63, 59,* 64,* 67*
6	A*0301		B*1402	B*4701		B 39, 61, 65, 27, 55, 37, 54, 56, 67, 73, 70,* 71,* 72,* 18,* 50,* 75,* 62*
7	A*3101	A*6901	B*0702	B*5501	A 68, 29, 33, 74, 30	B 54, 56, 42, 81, 67,* 39,* 64*

Fig.1 - An example of HLA matching between recipient and donor

There are more tests which are used to review and record the health of the donor (Hepatitis, HIV, Blood tests, X-rays, among many others). If during the tests it is found that the donor has a particular disease, then the organ could be used in patients with the same type of disease and blood type if the doctors agree. In the case of children, they can only accept organs from another child, or small or thin people.

4.2. Post-surgery related information

After the transplant occurs, the recipient patient undergoes an immunological suppressor treatment to avoid a rejection of the organ for the rest of his/her life or until the organ stops working (an average time of 10 yrs. for cadaveric donors, and 20-25 yrs. from living donors), forcing the patient to return to the 'waiting list', which only accepts people until 65 yrs. old, but there are some programs within the European Union who manage older patients. The patient stays in the hospital for a month and then returns depending on their condition (ex. Every 3 months), to check for antibodies or crossmatch and the sample cells from a donor are kept in liquid nitrogen within deep freezers in order to preserve them. It could also be that the patient experiences a rejection of the organ, as most of them occur during six

months after transplantation, but it can also occur several years later, and early treatment can help to reverse the rejection in most cases (UCSF, 2019). This relates to an interesting point as the information related to both the organ donor and recipient must be kept recorded and intact for a long period of time; potentially could have a conflict with GDPR requirements.

4.3. Electronic record systems handling as part of the transplant life cycle

Expiration of an organ is mostly of a few hours and therefore the organ transplantation needs to be executed within a window of time. A form of audit trail of all organs available and their respective journey through supply chain seems critical. As part of healthcare computing and record management standards, the European Federation for Immunogenetics addresses that a hospital laboratory must "Document each step in the processing and testing of patient specimens to assure that accurate test results are recorded", and that laboratory records must maintain depending on local regulations the following records:

- Logbooks
- Worksheets, that must clearly identify:
    - Sample tested
    - Reagents used
    - Methods used
    - Test performed
    - Date of the test
    - Person performing the test
    - Summary of results obtained
- All donor and patient related recorded information

It also specifies that that "Records may be only saved in computer files, provided that back-up files are maintained to ensure against loss of data" (EFI, 2017). Likewise, the European Health Committee of the Council of Europe, as part of their guidelines on standards required for quality assurance that must be achieved on services of transplantation of human organs, requires for hospitals to implement a "computerised record-keeping system that ensures the authenticity, integrity and confidentiality of all records but retains the ability to generate true paper copies"

with their hardware and software regularly checked to ensure they are reliable (Council of Europe Publishing, 2004). Similarly, the Foundation for the Accreditation of Cellular Therapy (FACT), as part of an extensive explanation of its standards on electronic record management and their validation, stipulates that “For all critical electronic record systems, there shall be policies, Standard Operating Procedures, and system elements to maintain the accuracy, integrity, identity, and confidentiality of all records”. It includes several detailed standards than point out the necessity of identifying any individual who interacts with record entries: from simple sign-in sheets to more complex systems that enable the tracking of record entries based on a user’s login-credentials. It also points out that the usage of any system whether it is built in-house or commercially acquired must be validated as the calculations must be correct under any circumstances, as they will affect the outcome of a decision related to the patient’s health (FACT, 2017). These guidelines also indicate that there should be a system that allows traceability from all steps and data performed and obtained during the transplantation cycle, and that it should be able to show the path each organ donation takes tracking them from the donor to the recipient or disposal and vice versa. The system also must respect the confidentiality of donors and recipients.

4.4. DNA sampling as part of the organ transplant life cycle

DNA samples are taken as part of the organ transplantation testing for both recipient and donor. In order to prevent that DNA samples are contaminated or maliciously replaced with a different one (for example someone within the hospital trying to bring an illegal organ to be used), a series of checkpoints are put in place. The first checkpoint is implemented is with the use of a method that detects variations in the DNA sampled called ‘HLA typing’.

The HLA typing method, as mentioned previously, is used to establish identity, parentage, and family relationship which helps to find out the appropriate matches for organ and tissue transplantation. According to guidelines and standards every blood sample that enters the laboratory takes a code number that is unique and characterizes this particular sample. Samples that are directed for DNA analysis (using molecular methodologies) take a unique code that is kept until the final results. The sample code is included in the final report for HLA typing (this is the second checkpoint) and the donor keeps at the laboratory the same code for further

analysis and for different procedures (as crossmatch with the patient). Following these rules, a mix up of the donor's DNA should never occur in the laboratory. The third and final checkpoint is the repetition of the HLA typing for donors and recipients, with new blood sample in order to confirm the results from the first sample.

4.5. Recording a DNA sequence in a public blockchain system.

The DNA or deoxyribonucleic acid is the hereditary material in humans and almost all other organisms - or a biological blueprint. The human genome is comprised about 3 billion base pairs (letters) which is the equivalent to 3.2GB of data (Elliot, Ryan, 2015).

Questions on cost storage of the data in a public blockchain, can be found with some calculations based on the paper "Ethereum: A secure decentralized generalized transaction ledger" (Wood, 2017) which most up-to-date blockchain blogs make reference to when making their case for storage costs in the Blockchain shows that in the Ethereum blockchain, one KB of storage will cost 0.032 ETH while a GB will cost 32,000 ETH (the price of ETH while writing this paragraph is at £116 GBP) , so to store 1GB of data will cost around £3.7 million pounds, which for any project type will be a prohibitive cost - even if the price per megabyte could round in the hundreds, to store 3.2GB of DNA data per patient it wouldn't make any sense. Hence why data storage off-chain is the option, more cost effective and cam comply GDPR privacy questions (if data were stored on-chain).

Most of the work related to DNA storage in a blockchain is in its infancy, and although there have been some proof of concept tests like the one performed by DNAtix in December 2017, where there was a transfer of the complete genome sequence of a virus over the Ethereum blockchain, this test only recorded about 5,400 base pairs which equates to 1,348 bytes (DNAtix, 2017)- this hardly grasps the range of the human genome, even with compression algorithms which can reduce the size to 700MB (some figures even mention the complete raw genome being in the +100GB range), making inefficient to store this amount of data with the current blockchain technology.

It needs to be understood that the blockchain technology was not conceived as a database for storing large files because it is computationally very expensive. For this purpose, data needs to be compressed and converted into a hexadecimal

format, and only the hash of the file in question should get recorded in the blockchain. Not all data needs to be recorded in the blockchain as in some cases it could potentially make the data unusable (ex. storing Medical image data) as blockchain transactions are slow to confirm, and is extremely slow when dealing with rich applications data flow as they might require many thousands of transactions per second.

Another issue will be the immutability of the blockchain which in some case will be a drawback for data storage of private-related information, as once data gets recorded it cannot be removed (ex. a patient photo-ID gets stored: even if it gets replaced by a different one, the previous data will reside within the blockchain forever can be seen by anyone). This point is key to the audit system as immutability provides the robustness to keep track of activity stored in the blockchain, so it is very important to understand the type of information that the system will be recording before putting it into production.

One additional drawback will be the storage capacity. If all medical and administrative related applications will keep their data in the blockchain, the size of the blockchain will grow very fast potentially exceeding hard drive capacity on each computer acting as a node becoming computationally very expensive.

5. GDPR Data Protection and Ethics

The General Data Protection Regulation is a European Union law implemented in May 2018 and requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory (GDPR EU, 2018). It includes seven principles of data protection and eighth privacy rights, these principles and rights must be implemented and ensured by all members of the EU and its enforcement carries heavy financial penalties for those organizations who incur on violations of the law - even if they are outside the European Union but handle data related to EU citizens.

The Information Commissioner’s Office (ICO), which is the UK's independent body set up to uphold information rights, provides a guide for data protection officers and other roles who have the responsibility for data protection on a daily basis, and covers Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR) as it applies in the UK (ICO, 2018). The GDPR requires that all organizations have in place appropriate organizational and technical measures

to secure personal data. One of these is encryption, as it is the most suitable electronic method at this moment for securing personal data. In this context, blockchain technology provides a secure and efficient method to create a tamper-proof log of transactions by the means of cryptographic hash functions on each block of the chain and by the use of digital signatures which are used for authentication, integrity of data and non-repudiation ensuring that the data recorded in the blockchain is valid.

5.1. The GDPR - blockchain paradox

The GDPR regulation brought the paradox on whether or not blockchain with its immutability attribute can function within the European Union legislation, and the topic is vastly discussed on the internet. Some groups (mostly from the United States) point that GDPR is fundamentally incompatible with how blockchain works in reality, implying that the European Union could close itself from how the future internet will be. It must be remembered that when the GDPR legislation was implemented, blockchain was mainly used for cryptocurrencies and wasn't taking into consideration this technology for industry use. In the current conditions, blockchain solutions potentially would need to be mutable by consensus or by a central administrator with the advantage that personal data could be deleted from the blockchain when someone requests the 'right to be forgotten' (one of the eight privacy rights of GDPR). The problem with this approach is that immutability is one of the core points in the existence of blockchain, and without it, it then will just be a common database.

GDPR legislation could benefit from the use of blockchain as it is a tool that actually can give better control to individuals of their own personal data; a good example will be through the use of 'Self Sovereign Identity' (SSI), a novel concept from the 'Sorvin Network', part of an open source project aimed to provide individuals with a digital identity "lifetime portable digital identity that does not depend on any central authority and can never be taken away" (Sorvin Foundation, 2018). But in the meantime, organizations are at risk of being non-compliant with the GDPR legislation, as personal identifiable information (PII) cannot be removed from the blockchain, so a different approach must be taken. That approach could be a hybrid solution with data help off-chain in data lakes or other traditional cloud cased models.

5.2. Ethics involved organ transplantation

Due to the fact that a living kidney transplantation can be performed with success using a kidney from a non-genetically related donor, adding to the long list of patients waiting for a transplant and the shortage of organs - including the uneven distribution of wealth in the world - this has created a scenario of organ harvesting that goes against the ethical framework followed by the medical transplant community and international organizations. The trafficking of organs and persons for the only purpose of commercialism and organ removal is forbidden by law in most countries, but unfortunately occurs in certain parts of the world (Toolbox Living Kidney Donation, 2016) and is increasing this criminal activity. Any institution that has a living donor program working within the ethical framework of organ transplantation guided by approved international standards must have all necessary regulatory infrastructure aligned with the European and UK legislations, and should also consider other safeguards that demonstrate the integrity of the program by any independent assessment prior to a transplant, that no reward has been offered (or given) that results in the donation of an organ, and that consent has been provided freely (no coercion to the donor has been made).

The NHS has also pledged to ensure that no UK resident participates in illegal transplantation related activities and will work in conjunction with the UK Health department and related authorities to prevent this type of ‘health tourism’ in the UK (NHS Blood and Transplant, 2017).

Having a model where everything can be recorded on blockchain and monitor audit control in all stages of organ donation makes complete sense for not just the audit, tracking, traceability but also to help deter criminal behaviours . The smart contracts will approve all milestones and consent and help safeguard ethics.

5.3. Evaluation of Blockchain and GDPR compatibility

The objective needs be addressed as part of the paradox between GDPR and blockchain: while GDPR was being created, its main target was conventional databases but not emergent technology such as blockchain. GDPR has among its privacy rights the concepts of ‘right to access information related to you’, ‘the right to be forgotten’, ‘the right to data portability’ and ‘the right to make companies edit-

correct-change information about you', while blockchain brings with it a some of its strongest points which are immutability and transparency.

There are some similarities between them, and both aim to provide a greater transparency on data and at the same time there are some important differences, the critical one being related to the immutability of blockchain and the rights that GDPR gives to users in order to erase, delete or add their personal identifiable information. GDPR requires user's identity but blockchain prefers anonymity, and as mentioned before, GDPR is focused more in centralized systems or common databases rather than decentralized like blockchains. Most of the GDPR regulations deal with personal data that has already being recorded - as there has been public outcry by knowing that certain social media companies have been collecting and monetizing people's data without their consent; and GDPR requests the users to agree to share their personal information, while blockchain for example of cryptocurrencies never deals with personal data. But blockchain uses public keys which are used to identify who creates a transaction and it potentially be that they could be treated as personal data by GDPR because they are connected to specific users - at this moment this has not been discussed in a court of law, so there is not a clear answer.

Many blockchain companies and consortiums are working to deal with this regulation taking diverse paths, as the pressure to comply with GDPR (and not get fined up to 4% of their annual worldwide revenue) increases. One way could be to issue a legal agreement between all the participants from a permissioned blockchain on which it will be agreed not to export the personal data in question, use it or copy it to an end user application or system (although the information could never be removed); this will need to be reviewed from a regulator point of view. Another method could be to improve the anonymization of information within blockchain in order to be compliant, this however requires more investment and testing.

Most recently in July 2019, the European Commission published a report regarding the impact of the EU data protection rules and how its implementation can be improved. The report shows that member states and businesses are developing a compliance culture and that its citizens are becoming more aware of their rights regarding their personal data. There is also a study performed by the European Parliamentary Research Service aimed to identify whether distributed ledgers be

squared with European data protection law; it points out that one of the main divergencies between GDPR and blockchain systems have is that GDPR assumes that data can be modified or erased to comply with its regulations, but blockchain makes these changes extremely difficult (or economically inviable) and this ensures the integrity of the data thus increasing the trust in the network, with the additional uncertain definition of the ‘erasure’ clause in its Article 17. The study concludes that it will be easier for permissioned or private blockchains to comply with the legal requirements of GDPR and also explains that it is not possible to assess the compatibility between GDPR and blockchain technology. It highlights however that the use of blockchain provides benefits from the data protection perspective, also offers several suggestions on how blockchains could get more legal certainty based on the interpretation of certain elements of the GDPR, and recommends that interdisciplinary research to explore how technical design of blockchains and their governance models could be adapted to GDPR requirements (Euro parliament, 2019).

6. Organ Supply Chain Framework

The scope to create a blockchain framework to manage the lifecycle of organ transplantation is both necessary for efficiency, ethics, transparency and critical to ensure supply chain can manage effectively the many moving components. This will further protect against any contamination and criminal behaviour and safeguard the provision that are both excluded any entry. The framework is recommended to deploy an applied methodology that provides the basis of mandatory requirements/compliance that usually encompasses a cyber security maturity model (CSMM). This will ensure that organisations that require to be part of the blockchain organ transplant supply chain fully understand and comply with compliance regulations and are frequently audited to ensure they are up to date and are following the objectives and requirements set out for when agreements to join take place.

Adopting a CSMM is a matter of selecting what is best suited to this type of supply chain. The same can be said regarding type of blockchain which must be able to operate in a distributed way where the application services involved run on multiple hosts and are not dependent on a centralised authority. Selecting the consensus mechanism is a similar exercise and for the purposes of this healthcare scenario

the PBFT consensus mechanism protocol is recommended. The PBFT pilot, as long it runs with less than 100 nodes, can offer 1000 transactions per second with a small payload size. This is considering that health records within blockchain will manage only data text, while it can also manage a good percentage of rogue nodes. For the blockchain model to be able to reach a fast throughput, the number of nodes in blockchain needs to be limited in order that it must be able to provide an efficient auditability and transparency of immutable information. Also, to be able to comply with data privacy regulations, the system must offer control of data access and anonymization of personal health related information.

The audit log process of the system should have also high throughput in order to manage the large number of log transactions and be able to integrate with existing systems with minimal changes or updates in the overall design and should be able to manage transactions of diverse sizes, as these might vary from between systems. The audit process will also provide a time stamped transaction sequence along with an audit trail to verify all transactions coming from each node and for stakeholders, while its architecture should be designed to be modular as well as service oriented so different types of applications can interact and benefit from it. Regarding security, the system will be able to prevent and neutralize any data tampering at its source. As it potentially will interact with other systems such as electronic health record systems, it will integrate its blockchain data transmission activities smoothly for a secure exchange of data, and have the feature of search and retrieval capability to retrieve any set of desired transactions with the length and time of search can be setup; this feature must be quick and responsive to ensure audits can be performed in real time. With regards to GDPR compliancy, some of the reviewed solutions do not get involved in the topic, others make the assumption that organizations who use the system are already compliant, and one offers a service to be ‘GDPR compliant’.

The proposed framework is based on theoretical design of an audit and tracking system based on blockchain technology supported by smart contracts with the aim to assist healthcare institutions to keep track and audit the organ transplant data that is recorded as part organ matching related activities. The proposed audit system should count with several features such as been able to convert audit log data to a blockchain compatible format that will be distributed among peers of the blockchain network. It should also have data integrity logic in order to have record

authenticity. From the security point of view, it should prevent rogue nodes from changing their transaction timestamps, and as part of a private-permissioned blockchain it should count with provisioned access control to selected users via an access control mechanism. This should allow auditability and transparency of records along with an end to end tamper-evident audit trail, proof of compliance, integrity and time stamp for authentication of transactions.

The following diagram shows the idea of the proposed blockchain based audit system and although a high-level design.

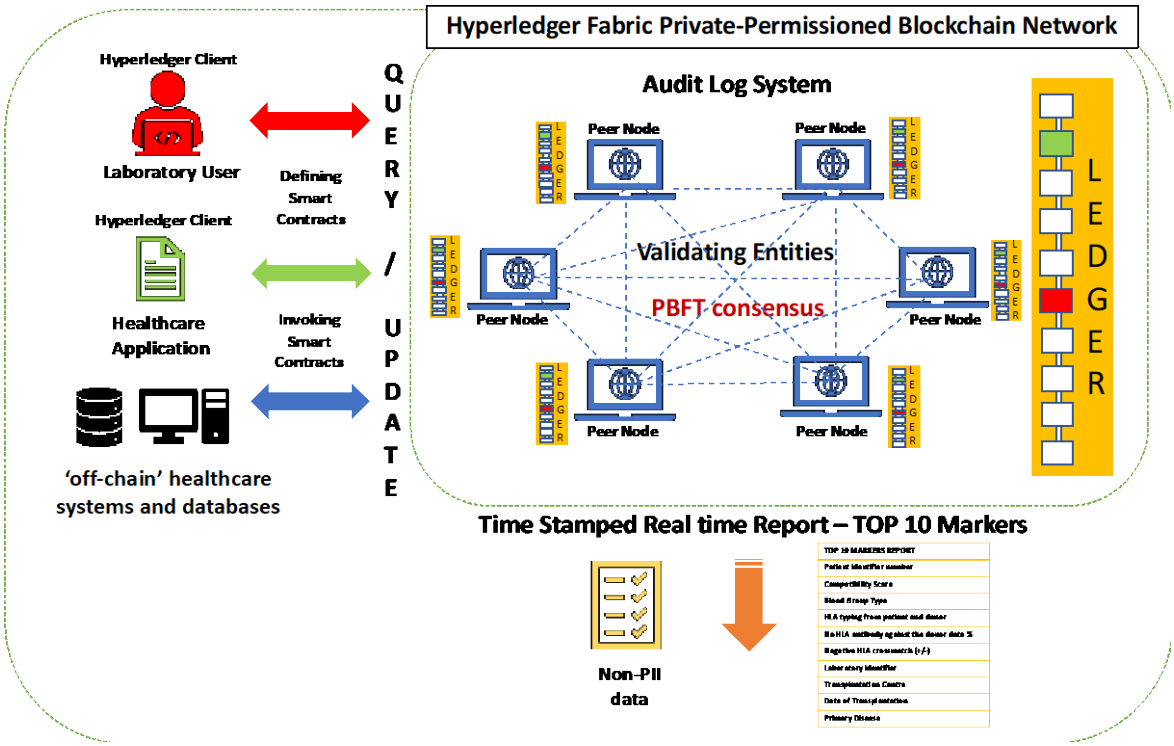

Fig. 4 - Proposed Blockchain Audit System

It is recommended that further studies be carried out to test and evaluate a Hyperledger installation with PBFT along another consensus mechanism that can compensate the needs of this protocol when having more than a hundred nodes in the blockchain, along with different sizes of data load in order to evaluate the maximum size of data where throughput gets diminished in order to explore different performance bottlenecks and tune-in the system.

Due to the fact that the organ transplantation is extremely complex because of the different types of organs and their transplantation protocols, it can be recommended

to gather available detailed information from the NHS transplantation healthcare centres based in the UK, showing per type of organ and evaluate what type of information needs to be recorded within the blockchain. Also, to perform tests with real life data, this with the goal to provide precise information that can be then shown as part of the reports. With the same idea in mind, it will be interesting to see how can this blockchain system can connect to a 'federated' blockchain model, so testing in that way are needed. From the medical side and in order to assure that the proposed system is used in a safe environment, a legal framework surrounding the activities with organ donations against unacceptable practices like organ trafficking, needs to be in place.

7. Conclusion

It is clear that organ transplant and supply chain needs some form of audit and tracking control that can help secure and maintain accuracy, ethics and transparency. Blockchain and its unique attributes can help provide this mechanism to further secure data and patient safety. It can also help deter the behaviours that has attracted both the criminal enterprise and desperation from individuals looking to illegally participate in selling their organs and those donors looking to procure.

It can also help post donor analysis of failures that occur and track and trace the origins as to what were exact reasons (in case the organ was not correct match, contaminated etc). Also, with these questions arising regarding DNA contamination. Adopting the right type of blockchain for organ supply chain is key and storing the data off-chain is an important consideration for cost effectiveness and privacy. Mixing the right type of cyber security maturity model will further enhance the potential for efficient compliance and ensure those that enter the supply chain are validated and continually audited with consequences for repeated failures to comply.

References

101 Blockchains (2018). Consensus Algorithms: The Root Of The Blockchain Technology. [online] Available at: https://101blockchains.com/consensus-algorithms-blockchain/ [Accessed 19 Dec. 2019].

101 Blockchains (2018b). Hyperledger vs Corda R3 vs Ethereum: The Ultimate Guide. [online] Available at: https://101blockchains.com/hyperledger-vs-corda-r3-vs-ethereum/ [Accessed 7 Nov. 2019].

Abboud, O., Abbud-Filho, M., Abdramanov, K., Abdulla, S., Abraham, G., Abueva, A.V., Aderibigbe, A., Al-Mousawi, M., Alberu, J., Allen, R.D. and Almazan-Gomez, L.C. (2008). The declaration of Istanbul on organ trafficking and transplant tourism. *Clinical Journal of the American Society of Nephrology*, *3*(5), pp.1227-1231.

Agbo, C., Mahmoud, Q. and Eklund, J. (2019). Blockchain Technology in Healthcare: A Systematic Review. Healthcare, 7(2), p.56.
CoinDesk. (2019). How to Mine Ethereum - CoinDesk. [online] Available at: https://www.coindesk.com/information/how-to-mine-ethereum [Accessed 7 Sep. 2019].

Ahmad, A., Saad, M. and Mohaisen, A. (2019). Secure and transparent audit logs with BlockAudit. Journal of Network and Computer Applications, [online] 145, p.102406. Available at: https://www.sciencedirect.com/science/article/pii/S1084804519302401 [Accessed 7 Jan. 2020].

Ambagtsheer, F. (2020_. Combating Human Trafficking for the Purpose of Organ Removal: Lessons Learned from Prosecuting Criminal Cases. *The Palgrave International Handbook of Human Trafficking*, pp.1733-1749.
Ambagtsheer, F., Zaitch, D. and Weimar, W., 2013. The battle for human organs: organ trafficking and transplant tourism in a global context. *Global Crime*, *14*(1), pp.1-26.
Bagheri, A. and Delmonico, F.L., 2013. Global initiatives to tackle organ trafficking and transplant tourism. *Medicine, Health Care and Philosophy*, *16*(4), pp.887-895.

Arnold, A. (2018). Is Blockchain The Answer To A Better Healthcare Industry?. [online] Forbes.com. Available at: https://www.forbes.com/sites/andrewarnold/2018/08/26/is-blockchain-the-answer-to-a-better-healthcare-industry/#f839edf75a8b [Accessed 16 Aug. 2019].

Bitcoin.it. (2018). Majority attack - Bitcoin Wiki. [online] Available at: https://en.bitcoin.it/wiki/Majority_attack [Accessed 26 Nov. 2019].

Blockchain Consensus Algorithms & Mechanisms: Startup Guide For Beginners. (n. d.)[online] Available at: https://www.developcoins.com/blockchain-consensus-algorithms [Accessed 1 Oct. 2019].

Blockchain council. (2019). Best Programming Languages to Build Smart Contracts. [online] Blockchain-council.org. Available at: https://www.blockchain-

council.org/blockchain/best-programming-languages-to-build-smart-contracts/ [Accessed 7 Dec. 2019].

Buck, J. (2017). Blockchain Oracles, Explained. [online] Cointelegraph. Available at: https://cointelegraph.com/explained/blockchain-oracles-explained [Accessed 29 Nov. 2019].

Budiani-Saberi, D.A. and Delmonico, F.L. (2008). Organ trafficking and transplant tourism: a commentary on the global realities. *American Journal of Transplantation*, *8*(5), pp.925-929.

Caulfield, T., Duijst, W., Bos, M., Chassis, I., Codreanu, I., Danovitch, G., Gill, J., Ivanovski, N. and Shin, M. (2016). Trafficking in human beings for the purpose of organ removal and the ethical and legal obligations of healthcare providers. *Transplantation direct*, *2*(2).

Caplan, A., Dominguez-Gil, B., Matesanz, R. and Prior, C. (2009). Trafficking in organs, tissues and cells and trafficking in human beings for the purpose of the removal of organs. *Joint Council of Europe/United Nations Study*.

Coincap.io. (2017). CoinCap.io | Reliable Cryptocurrency Prices and Market Capitalizations. [online] Available at: https://coincap.io [Accessed 20 Aug. 2019].

ConsenSys. (2019). General Philosophy - Ethereum Smart Contract Best Practices. [online] Github.io. Available at: https://consensys.github.io/smart-contract-best-practices/general_philosophy/ [Accessed 15 Nov. 2019].

Council of Europe. (1997). Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. *Oviedo: COE*.

Corda. (2019). Corda | Open Source Blockchain Platform for Business. [online] Available at: https://www.corda.net [Accessed 8 Oct. 2019].

Council Of Europe Publishing. (2004). Guide to safety and quality assurance for organs, tissues, and cells. 2nd ed. Council of Europe Publishing: The Council of Europe.

Foundation for the Accreditation of Cellular Therapy. (2019). COMMON STANDARDS for CELLULAR THERAPIES. [online] http://www.factwebsite.org. Available at: http://www.factwebsite.org/WorkArea/DownloadAsset.aspx?id=1970.

Doran, G. T. (1981). "There's a S.M.A.R.T. way to write management's goals and objectives". Management Review. 70 (11): 35–36.

Gartner (2019). Gartner blockchain hype cycle 2019: 60% CIOs to adopt within 3 years - Ledger Insights. [online] Ledger Insights. Available at: https://www.ledgerinsights.com/gartner-blockchain-hype-cycle-2019/ [Accessed 24 Dec. 2019].

DNATIX. (2017). DNA Sequences on the Blockchain. [online] DNAtix - The secure platform for Genetics. Available at: https://www.dnatix.com/dna-sequences-on-the-blockchain/ [Accessed 8 Dec. 2019].

Dragonchain. (2019). Dragonchain | Blockchain as a Service. [online] Available at: https://dragonchain.com [Accessed 22 Oct. 2019].

Ekblaw, A., Azaria, A., Halamka, J., Lippman, A. and Vieira, T. (2016). A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data. [online] MIT Media Lab. Available at: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf [Accessed 25 Nov. 2019].

Elliott, T.A. and Gregory, T.R. (2015). Do larger genomes contain more diverse transposable elements? BMC Evolutionary Biology, [online] 15(1). Available at: https://bmcevolbiol.biomedcentral.com/articles/10.1186/s12862-015-0339-8 [Accessed 7 Jan. 2020].

English, E., Davine, A. and Nonaka, M. (2018). Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry. [online] Chamber of Digital Commerce. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1TH5G [Accessed 12 Oct. 2019].

E-estonia briefing centre. (2019). About us — e-Estonia. [online] e-Estonia. Available at: https://e-estonia.com/about-us/ [Accessed 15 Dec. 2019].

European Parliament. (2010). EUR-Lex - sp0008 - EN - EUR-Lex. [online] Europa.eu. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:sp0008 [Accessed 7 Dec. 2019].

European Federation for Immunogenetics. (2018). Standards for Histocompatibility & ImmunogeneticsTesting Version 7.0. Standards and Quality Assurance Committee, Available at: https://efi-web.org.

European Union. (2019). FAQ - GDPR.eu. [online] GDPR.eu. Available at: https://gdpr.eu/faq/ [Accessed 28 Nov. 2019].

European Parliament. (2019). Blockchain and the General Data Protection Regulation. [online] Available at: https://www.mybib.com/#/projects/4K0O6v/citations/new/webpage [Accessed 15 Dec. 2019].

European Union - Working Group on Living Donation. (2016). Toolbox Living Kidney Donation.
NHS Blood Transplant (2017).

Gill, J.S., Goldberg, A., Prasad, G.V., Fortin, M.C., Hansen, T.B., Levin, A., Gill, J., Tonelli, M., Tibbles, L.A., Knoll, G. and Cole, E.H. (2010). Policy statement of

Canadian Society of Transplantation and Canadian Society of Nephrology on organ trafficking and transplant tourism. *Transplantation*, *90*(8), p.817.

Goquorum.com. (2019). Home. [online] Available at: https://www.goquorum.com [Accessed 9 Oct. 2019].

Fernández-Caramés, T.M. and Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. [online] www.semanticscholar.org. Available at: https://www.semanticscholar.org/paper/A-Review-on-the-Use-of-Blockchain-for-the-Internet-Fern%C3%A1ndez-Caram%C3%A9s-Fraga-Lamas/02458904f9bd718bd8c6a1a36e9847ad83b0410b [Accessed 4 Nov. 2019].

Genomes.io. (2019). [online] Genomes.io. Available at: https://genomes.io [Accessed 11 Dec. 2019].

Holmes, P., Rijken, C., D'Orsi, S., Esser, L., Hol, F., Gallagher, A., Greenberg, G., Helberg, L., Horvatits, L., McCarthy, S. and Ratel, J. (2016). Establishing trafficking in human beings for the purpose of organ removal and improving cross-border collaboration in criminal cases: recommendations. *Transplantation direct*, *2*(2).

Hu, Y., Manzoor, A., Entertainment, R., Thilakarathna, K. and Data61-Csiro, G. (2019). Blockchain-based Smart Contracts - Applications and Challenges. [online] Available at: https://arxiv.org/pdf/1810.04699.pdf [Accessed 30 Sep. 2019].

Hyperledger. (2019). Hyperledger – Open Source Blockchain Technologies. [online] Available at: https://www.hyperledger.org [Accessed 7 Oct. 2019].

Jafar, T.H. (2009). Organ trafficking: global solutions for a global problem. *American Journal of Kidney Diseases*, *54*(6), pp.1145-1157.

IBM.COM. (2019). The Founder’s Handbook Your guide to getting started with blockchain Edition 2.0. [online] Available at: https://www.ibm.com/blockchain/platform [Accessed 30 Nov. 2019].

Information Commissioner’s Office. (2018). Guide to Data Protection. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/ [Accessed 3 Dec. 2019].

Ixxo.io. (2019). IXXO | Digital and Financial Assets Trusted Exchange Through Blockchain Infrastructure. [online] ixxo.io. Available at: https://github.com/ixxo-io [Accessed 20 Dec. 2019].

James, A. (2018). 92% of Blockchain Projects Have Already Failed, Average Lifespan of 1.22 Years - Bitcoinist.com. [online] Bitcoinist.com. Available at: https://bitcoinist.com/92-blockchain-projects-already-failed-average-lifespan-1-22-years/ [Accessed 5 Dec. 2019].

Mikulic, M. (2017). Healthcare blockchain adoption rate worldwide 2017 | Statista. [online] Statista. Available at:

https://www.statista.com/statistics/759208/healthcare-blockchain-adoption-rate-in-health-apps-worldwide/ [Accessed 18 Aug. 2019].

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. [online] Bitcoin.org. Available at: https://bitcoin.org/bitcoin.pdf [Accessed 18 Aug. 2019].

NHS UK. (2019). Statistics about Organ Donation. [online] NHS Organ Donation. Available at: https://www.organdonation.nhs.uk/helping-you-to-decide/about-organ-donation/statistics-about-organ-donation/ [Accessed 9 Dec. 2019].

Nhsbtdbe.blob.core.windows.net. (2019). Organ Donation and Transplantation - Activity figures for the UK as at 8 April 2019. [online] Available at: https://nhsbtdbe.blob.core.windows.net/umbraco-assets-corp/15720/annual_stats.pdf [Accessed 17 Aug. 2019].

Office for Civil Rights (OCR). (2015). 187-What does the HIPAA Privacy Rule do. [online] HHS.gov. Available at: https://www.hhs.gov/hipaa/for-individuals/faq/187/what-does-the-hipaa-privacy-rule-do/index.html [Accessed 5 Dec. 2019].

Pietrobon, A. (2016). Challenges in Implementing the European Convention against Trafficking in Human Organs. *Leiden Journal of International Law*, *29*(2), pp.485-502.

Preventing Organ Trafficking and Transplant Tourism in the UK. (2017). [online] NHS Blood Transplant, p.9. Available at: https://nhsbtdbe.blob.core.windows.net/umbraco-assets-corp/4331/79th-meeting-board-report.pdf [Accessed 29 Nov. 2019].

Rice, J. (2019). Tachyon Burst: Genomes Wants To Put You On The Blockchain. Yes, You. | Crypto Briefing. [online] Crypto Briefing. Available at: https://cryptobriefing.com/genomes-blockchain-data-privacy/ [Accessed 2 Dec. 2019].

Schrans, F. (2018). Writing Safe Smart Contracts in Flint MEng Individual Project. [online] Imperial College London. Available at: https://www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/1718-ug-projects/Franklin-Schrans-A-new-programming-language-for-safer-smart-contracts.pdf [Accessed 26 Nov. 2019].

Shorthouse, D. and Morrissey, M. (2018). GDPR Compliance using KSI ® Blockchain Guardtime Whitepaper on VOLTA -its KSI ® blockchain-based solution for GDPR. “Guardtime’s VOLTA product presents a path to GDPR certification that really stands out in today’s marketplace.” [online] Guardtime, p.8. Available at: https://m.guardtime.com/files/guardtime-whitepaper-volta-v2.pdf [Accessed 16 Dec. 2019].

Steering Committee of the Istanbul Summit. (2008). Organ trafficking and transplant tourism and commercialism: the Declaration of Istanbul. *The Lancet*, *372*(9632), pp.5-6.

Szabo, N. (1994). Smart Contracts. [online] Hum.uva.nl. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [Accessed 29 Nov. 2019].

The Sovrin Foundation. (2018). Sovrin TM: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust A White Paper from the Sovrin Foundation. [online] The Sovrin Foundation. Available at: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf [Accessed 7 Dec. 2019].

UK Parliament. (2018). POSTbrief number 28. [online] Available at: https://www.parliament.uk/mps-lords-and-offices/offices/bicameral/post/post-publications/postbriefs/ [Accessed 7 Oct. 2019].

UK NEQAS. (2017). Home - UK NEQAS | External Quality Assessment Services. [online] UK NEQAS. Available at: https://ukneqas.org.uk [Accessed 27 Nov. 2019].

US Department of State (2019). 'Trafficking in Persons Report June 2019'. [Online].
Available at: https://www.state.gov/wp-content/uploads/2019/06/2019-Trafficking-in-Persons-Report.pdf [Accessed 2 Feb 2020]

University of California San Francisco. (2010). Transplant Surgery - Kidney Transplant. [online] UCSF.edu. Available at: https://transplantsurgery.ucsf.edu/conditions--procedures/kidney-transplant.aspx [Accessed 14 Dec. 2019].

Valenta, M. and Sandner, P. (2017). FSBC Working Paper: Comparison of Ethereum, Hyperledger Fabric and Corda. [online] Explore-ip.com. Available at: http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf [Accessed 24 Oct. 2019].

WHO. (2004). Organ Trafficking and Transplantation Pose New Challenges. [Online].
Available at: https://www.who.int/bulletin/volumes/82/9/feature0904/en/index1.html [Accessed 2 Feb 2020].

WOOD, G. (2017). ETHEREUM: A Secure Decentralised Generalised Transaction Ledger EIP-150 REVISION. [online] Available at: http://gavwood.com/Paper.pdf [Accessed 22 Dec. 2019].

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018). NISTIR 8202 - Blockchain Technology Overview. [online] Nvlpubs.nist.gov. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf [Accessed 24 Aug. 2019].

YEUNG, K. and GALINDO, D. (2019). Why do Public Blockchains Need Formal and Effective Internal Governance Mechanisms? European Journal of Risk Regulation, 10(2), pp.359–375.

Zawicki, K. (2018). Keyless Signature Infrastructure (KSI): Blockchain Technology for the Defense Industry. [online] GuardTime Federal. Available at: https://potomacinstitute.org/images/VITAL/2018-08-16-KSI---Blockchain-Tech-for-DoD.pdf [Accessed 8 Dec. 2019].