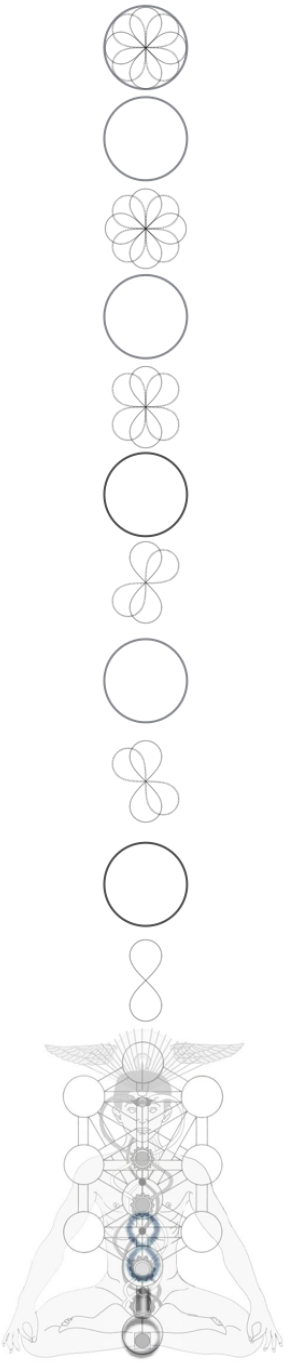
Doctelligence: White Paper

By Abraham Nash



Doctelligence: A Decentralised Intelligence Health Network

Abraham Nash
doctelligence.org

Abstract: Doctelligence enters participants into a decentralised intelligence health network via sovereign authentication architectures using public key identities in the setup of healthcare provision. The main participants are health users, spaces, providers and systems. The network's root infrastructure merges an architecture of user permissioned personal health records data access into a real world layer of health space nodes to host interoperable provision. An ERC-20 token accesses federated learning protocols on-chain for systems to train algorithm models on users personal health records for providers to embed into updated models of health care practice. Users receive token transactions as incentive to participate in federated learning rounds with a long-term roadmap to developing cryptographic-based insurance solutions.

1. Introduction

Doctelligence enables the setup of decentralised health care provision via a public blockchain ledger using public key cryptography issuing private/public key pairs. It is built on the ethereum proof of stake (PoS) chain solidity coded smart contracts to incorporate self-sovereign identification methods by authenticating key participants into a user-centric healthcare setup [1].

A root architecture of open source personal health records permissions acess enables users to enter into and develop their own decentralized health care networks of practice all through a distributed layer of real world space nodes which act as non-competitive, low entropy carriers to host real world provision. On-chain policies code for local licensing/credentialing mechanisms for physicians and premises which govern the region to allow a user-based sovereign setup of healthcare provision and services. These mechanisms allow the network to integrate across any region, to any healthcare system, expanding any model of health care practice based on user-centric public/private key-based interaction and request-based mechanisms.

Health systems (i.e. AI startups, AI- Clinical Decision Support Systems) are provided entrance into a decentralized healthcare network using ERC-20 tokens to train their models (i.e. algorithms) on federated learning protocols distributed on-chain. Users opt-in to federated learning protocols via permissions held on-chain using smart contracts that are called to their personal health record databases held on local devices (i.e. laptop, mobile) [2]. Systems embed their algorithm models into real world models of health practice (i.e. clinical care pathways) as health care professionals seek to combine supportive technologies, such as decision systems, into the provision of health care to run on users' personal health records. A shift in focus to the deliverable scalable models of healthcare is supported, with new technologies to maximise efficiency, reduce cost, and build cumulative provision across a decentralised intelligence health network.

These mechanisms lay the basis for a learning health system creating a return of value in the form of new systems technologies input into updatable, adaptable and scalable models of healthcare practice. Token transactions are passed directly into users' digital wallets to fund access to healthcare provision with a roadmap to developing cryptographic-based insurance solutions. A long-term roadmap seeks to remove entry barrier-thresholds to healthcare access and lays the foundations for universal health coverage that would not, for example, rely on government subsidy.

A model-view-controller pattern makes distinct the role of the network as server components and user interface applications connect to distributed marketplaces and enter participants into the setup of sovereign healthcare provision. A metamask (and/or other blockchain software) enables entities to link the symbol (o=∞) as a portal into the blockchain to access the network.

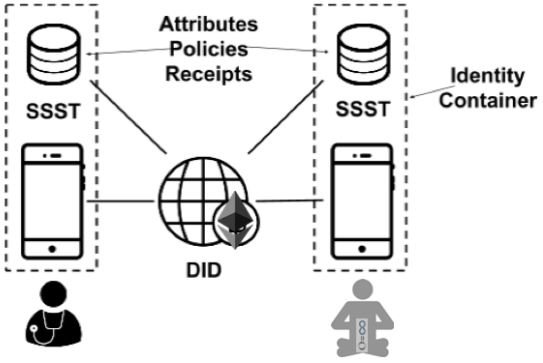
2. Self-Sovereign Identity (Root Layer)

A user-centric, self-sovereign architecture, uses a non-repudiate method of authentication in the set-up of health care practice. The primary architecture centres on the relationships established between users-physicians and the setup of healthcare provision [1].

Public/private key-pairs link to participants identities stored on a public blockchain ledger [Ethereum]. A professional entity (i.e. physician) in control of their private key (i.e. eIDAS sense of non-repudiation of control) authenticates themselves into the network using a private key associated with a trusted reputation mechanism, such as federally accepted credentialing/licensing agents in healthcare ecosystems [HIE of One]. The secure elements participants are encouraged to use to establish oneself into the network are signing, encryption, payment keys and biometrics (i.e. fingerprint) via user interfaces [1].

A self-sovereign identity allows each entity to enter themselves into the decentralised health network using their local devices (i.e. phone, laptop). Users have the option to integrate sovereign, community and commercial-based servers (or cloud-based encrypted servers) to store and determine their interactions with on-chain policies depending on their preferences [1]. User Managed Access (UMA) authorisation servers, decentralised identities, on-chain policies, whitelists of federated ID providers, and privacy related server software (e.g. protected attribute stores, transaction receipt stores) are all suggestions for implementable server-based components to support the network. A basic user interface application to manage DID keys, biometric access controls and key recovery will be made publicly available as well as online self-sovereign support technology (SSST-built from source) to guide adoption of the network by commercial vendors [1].

An open-source personal health record system (i.e. NOSH) is integrated into the design of the network and is integral to the design of a decentralised health network. Users, providers, spaces and systems interact as participants with their own public/private key pairs which utilise smart contracts that record affinities, authenticate participants, specify permissions of personal health records access, as well as to access wider services in the provision of healthcare [2, 3]. All entities can use different self-sovereign technology to support and/or personalise their security, privacy and economic interests in utilising the network [1].



3. Personal Health Record (Root Layer)

An open-source personal health records systems (i.e. NOSH) enables providers to connect to users (i.e. patients) personal health records to read and write into during the provision of healthcare. A single health record is stored on users' local databases held on local devices (i.e. laptop, mobile) over their lifetimes [2]. A clinician accesses users' personal health records through a one-way API portal into local databases held on user devices (i.e. laptops, mobile) as governed by on-chain access-permissions specified by users [1, 2]. A baseline FHIR standard is incorporated into the smart contract to validate FHIR API access standards in accessing users' personal health records in the network [3].

The personal health record access-permissions are recorded on an *affinity* smart contract which stores a status variable, indicating when access of a physician was established, and whether it has been approved by the user [3]; the *affinity* smart contract enables other entities/participants in the network to establish relationships. The acceptance, rejection or deletion of access is controlled by the user, though a provider can send requests and delete their affinities to users too. The *affinity* smart contract logs all user interactions and requests on the portal, e.g., what resource is shared or no longer shared with which provider by whom and when [3]. A joining healthcare professional (i.e. physicians) to an existing provider who has already established affinity to a patient can use a secure cryptographic mechanism called "sign then encrypt" to access a user's (patients) personal health record [4]. A request (i.e. by a provider) is cryptographically signed by the issuer (i.e. original physician) using their public/private key pair allowing the user to confirm identities of both the original and joining physician [3] . These access logs are structured as a mapping between user digital health identities (public encryption keys) and authorizations to custom-named access tokens [3].

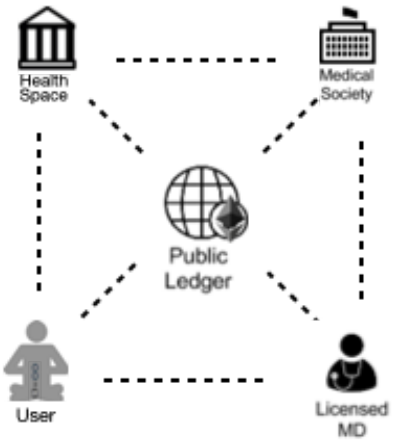
These secure access tokens are recorded in the smart contract for decentralized access and traceability; the smart contract maintains an immutable timestamped transaction log of all events related to exchanging and actually consuming these access tokens [3]. These logs include specific information regarding what access has been granted to which participant and by whom, who has consumed which token to access what part of the record and for what purpose, etc. A new pair of signing keys is generated for each entity and registers the public portion of signing keys alongside users' digital identities [3]. This design employs the users' digital health identities to encrypt content so that only users holding the correct digital identity private keys can decrypt the content to access pointers to users' personal health records stored on their databases (i.e. local laptop, mobile). In this way it satisfies usability criterion with pointers to personal health records stored in the form of access permissions on a decentralised blockchain [3]. Once an issuer's signature is certified, the user checks the blockchain contracts and verifies if the address issuing the request is allowed access to the query string. If the address checks out, it runs the query on the entity's preferred server which grants access to their local database (i.e. personal health record) and returns the result over to the client (i.e. API clinician-portal) [3].

Viewing permissions are recorded as encrypted pointers on the ethereum public blockchain [1, 3]. A data requestor's access to a resource can be approved or revoked at any time by the user as a state update in the smart contract where all permissions (i.e. reading, writing) are logged [3]. The *affinity* smart contract initialises a relationship between the user-physician (and other participants as necessary) to enable cryptographic access permissions to be set up on-chain and to develop the user's network. A *network* smart contract keeps a log of all user-physician affinities with any necessary meta-data so that users may create their own on-chain decentralised health networks. If a user were to lose their server or application-based components (i.e. user interfacing applications) then their decentralised health networks can be re-accessed through reconnecting to the blockchain in which their network survives on-chain. [3]. A variety of high level panels (i.e. JSON etc) have already concluded that separating access control from personal health record stewardship (cross-silo) is necessary to achieve interoperability at scale [1]. The network focuses solely on data access (cross-device) though access permissions can specify metadata detailing the potential for data-exchanges for basic purposes only if needed (i.e. auditing, research) [3].

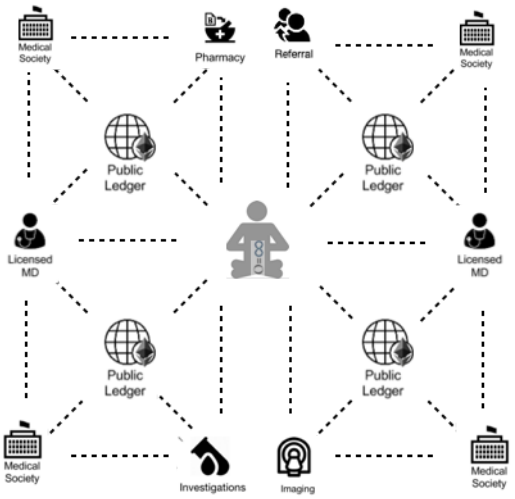
4. User (Real World Layer)

The use of sovereign identities in the network allows users to develop their own decentralised health networks and services. An *authentication* smart contract is linked to *affinity* to call authenticated entities when required, to authenticate professional roles in the network (i.e. spaces, physicians, systems). A time-limit may be set before re-authentication of identity is required to maintain access to users' personal health record [3]. This authentication process can be automated by server components interfacing with the smart contracts on-chain, and communicated to participants via user interfaces, to ensure affinities are established with authenticated participants only [1]. This architecture forms the basis of request and interaction mechanisms between participants which both prompt/inform the setup of healthcare.

A user-centric authentication architecture enables a user to set up health care provision using public/private key pairs in a sovereign manner. A user, physician, and space interact to set up healthcare without any participant relying on any institution [1]. Health provision is confirmed using a physician's licence authenticated via medical societies (or renowned third parties) using their blockchain based identities (i.e. public/private key-pairs). Premise (i.e. health space) is confirmed in a similar way via local licensing permissions of that jurisdiction (e.g. surgical premise). To ensure validity, the network will configure on-chain policies/protocols to enable participants to sync automatically with local governing regions to make use of trusted licencing/credentials via the *authentication* smart contract [3].



A step-by-step authentication sees physicians use their blockchain public/private key-pair to confirm their identities with a licensure/credentialing agent, who issues their identity-confirmed practice licence/credential [1]. The physician presents their authenticated licence to the user who in turn presents it to their desired premise i.e. space node. The space node confirms this licence separately with the licensing/credentialing agent before health care proceeds on premise. This process may be completed counter-clockwise to verify the licensure of the health space (i.e. for tele-robotic surgery) on premise. In practice, some steps may be automated by server components of each participant to confirm physician and premise credentials/licensure before the user completes the set-up of health care.

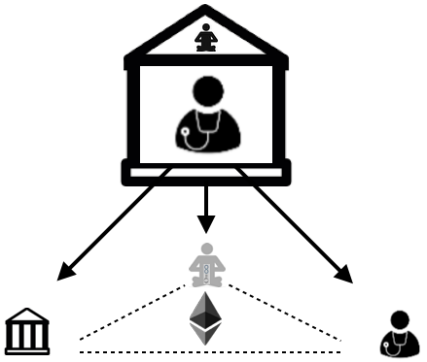


The interaction between wider healthcare services fundamental to healthcare provision are also facilitated by the same sovereign authentication architectures without any service relying on any institution or one another [1]; referrals, pharmaceutical, immunizations, medical investigations, imaging services, consent forms, and more. Services using their public/private key pairs connect using their servers to credentialing agents' servers in the same way to authenticate the public-key identities of physicians (or themselves) on-chain to confirm licensure/credentials [1]. Success will mean that no institutional or service-based entity has to trust another institutional identity to learn about another entity, as long as the jurisdiction they are in recognises the authority of a blockchain-based identity and reputation-based agent (e.g. medical society) [1].

The non-sovereign identity in this architecture reflects the nature of society in which governance is still present, in this case the licensure and credentialing agents of the real-world architecture. A decentralised intelligence network seeks to incrementally build toward a completely trust-less architecture for all relevant participants, rooted in a trust-less system (i.e. ethereum public blockchain) as a part of its long term roadmap. The network is designed to enable societal transition and involves bringing those licensure/credentials online with their own blockchain identities i.e. medical boards, medical-schools ete. However, a trustless public blockchain architecture still encircles the user with trusted entities remaining at the edges and may be replaced with sovereign blockchain identities over time.

5. Health Space (Real World Layer)

The decentralization of physical space is a useful concept to separate out the key functions of provision within a healthcare ecosystem, and in this case, a requirement to fully dissolve the health care institutional entity whilst maintaining access to facilities in space. As its own entity, a space node will have less inherent motives to act dishonestly in the network with it being separated from the data economy [5].

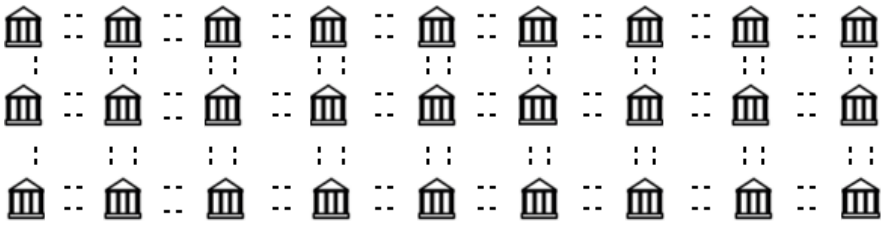


Health spaces are separated out as non-institutional entities, incentivised to develop as interoperable nodes with facilities to support diversified portfolios of healthcare practice (i.e. surgical, clinical etc). They receive their own public/private key-pair identities to interact with users, physicians, and systems in the hosting of healthcare provision. A diversified practice portfolio enables space facilities a robustness and immunity unto natural fluctuations in the growth and contraction of provider practices within a region. Decentralising the ownership of space provides access to provision for the expansion of decentralised provision and enables user-centric, self-sovereign setups of healthcare, as it eliminates the ability of institutional entities to preferentially block or select professionals (and their practices) from growing in a region.

Health space nodes use their own public/private key pairs to authenticate themselves into the network and to interact with participants (e.g. users). Space nodes provide individual, small and medium sized providers the opportunity to enter their models of health practice into a distributed network and do not involve themselves in the data economy. This encourages the development of interoperable facilities to host a diversified portfolio of individual, small and medium practices, responding to local demand, and providing practices the ability to access facilities in space across new populations. Health space broadens the capabilities of health care practice by enabling more advanced health systems to be utilised in health practice (e.g. advanced consultation equipment, telerobotic surgical facilities). Providers are able to focus on the expansion of their health care practices as accessed by users to their requested space (or node). The combination of public/private key pair request mechanisms within a distributed layer of space nodes lowers the associated risk and capital-costs associated with relocating or expanding a practice. A user makes use of their public/private keys in their local/regional locations to overcome limitations in the availability and choice of local provision to shape their own healthcare landscape either individually, or, as a part of their own communities.

Centralised provision, on the other hand, relies on limited user options of available practices through the acquisition of space and development of uniform models of health care practice alongside a growing scaled acquisition of health data economies to drive-out competition. Unfortunately, the trade off is ingenuity and a diversity in available practices within a territory in which ultimately, the user (i.e. patient) loses. Once such provision is bought-out institutions cement themselves in society as modern day lords reminiscent of the medieval European feudal system, posing as crown and high priest alike, hiding themselves behind the pry's of government subsidy and over-priced insurance premiums, pivoting with disposable nobles to perform their honorable duties, and where the people - who know no better - scour to and flee for protection in return for life-long servitude and non-negotiable financial fees. Meanwhile, the occasional merchenter (i.e. physician) is allowed to rise beyond their born status, higher than or equal to their families before them to buy more social prestige with the allure of nobility.

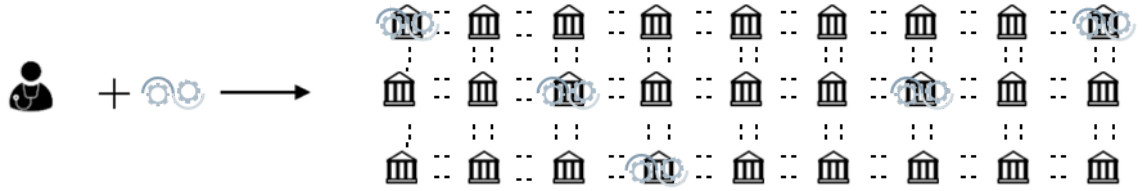
Individual, small and medium sized practices cannot hope to compete with large centralised institutions, despite their proposals for new, creative and competitive models of health care practice. And those practices which manage to do well often switch to focusing on income based capital in place of practice asset growth, which results in capping the market population by raising income based capital to cope with demand due to the inability to expand in space strategically acquired by centralised institutions. This reduces rather than increases access to provision and often results in distorted marketing tactics, geared toward scarcity and the elite, rather than abundance and the populous.



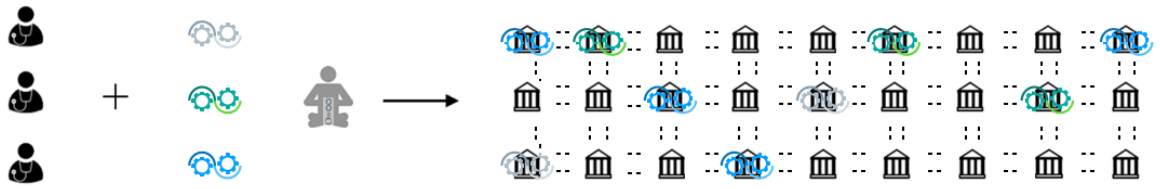
6. Health Provider (Real World Layer)

Users select their own providers in a decentralised health network using sovereign based-identities held on the blockchain with their public/private key-pairs. Users determine the access of physicians/providers and, determine who has access to their personal health records via a clinician portal ((i.e. API) held on local devices at minimum/or no cost to either participant (i.e. physician-user) [2]. An open-source personal health records system allows for more representative consensus and open dialogue in suggesting and/or making any updates to a system. In this setup, the privacy and security of health records is no longer the concern or responsibility of the provider who may instead return to focus on health care practice. The privacy of personal health records are handled on a public blockchain ledger that stores permissions, whereas, the individual security is distributed to the edges and is the responsibility of individual users and their devices.

Users interact with providers using private/public key request-based mechanisms to prompt set up of their own health care provision, bypassing the inertia of institutions [1]. These request mechanisms interact with professionals/providers and prompt practice to space nodes within users' desired regions. The models of practice of that provider are hosted by original physicians of the practice in-person or remotely, or by joining physicians of the practice who are licenced to authenticate within that region to host the models of that practice in-person or remotely. The original provider re-authenticates themselves using the *authentication* smart contract to request clinician-portal access for the joining physician through the *affinity* smart contract using their own public/private key-pairs; any authenticatable physicians who may host the model of practice within that facility in space may now be selected by the provider within the region, who are provided with access tokens for them to read and write into the users personal health record via the API clinician-portal gateway. A long term road map induces interoperable facilities in space and the capabilities for users to select care (i.e. tele-robotic surgery) in any one of 15 locations or more without displacing themselves or the physician.



Merit-based models are selected as a growing understanding between user-physicians as to the models of healthcare practice on offer, rather than individual physicians, and allows for a better discourse in the selection of healthcare provision. The network shifts the focus to reward successful practices on the basis of merit via adoption of models across distributed nodes in the network and allows individual, small and medium sized practices to grow, as prompted by user agency and the creativity of physicians/providers. Whereas previously, centralised healthcare facilities may be networked and communications between individual, small and medium sized practices may not have been established (or have the means to coordinate this) [3]. The provider may switch to focus on asset growth rather than income in order to expand their practice models, and to focus on engineering updated models of health care practice through embedding systems technologies into care pathways to develop updated and competitive, superior and cost-effective healthcare provision.



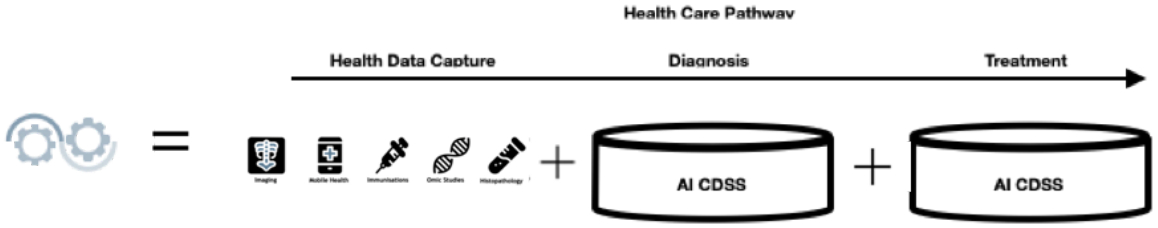
A user-centric sovereign selection of wider health care services (i.e. pharmacy, referrals, imaging services etc) as previously illustrated further supports the physicians ability to steer informed healthcare (i.e. cost-effective options, efficiency, up-to-date technologies and services) based on their own insights and knowledge. This allows a physician to practice more freely and guide the user, whereas before, physicians could feel limited to enhance their patients experience due to the limitations imposed by the vested interests of centralised healthcare institutions and their partnering services.

Health care professionals/providers remain incentivised due to the reduced financial and administrative costs associated with existing health record systems coupled with the opportunity to grow practice across a distributed layer of health space nodes in the real world. The use of open-source personal health records offsets the costs of expensive health record systems, enables an open dialogue behind the designs of any implemented health records software, handles privacy concerns via the network, offsets the security concerns associated with large electronic health records database and benefits from the ability to specify for integrated functions of health systems (i.e. AI-Clinical Decision Support). The user-physician interaction, as well as health system functions (i.e. decision support), benefit from the users personal health data being located in one location (i.e. user local devices/databases) in the decentralised intelligence health network [7]. Healthcare practice expansion will focus in the outpatient/day-case environments to begin with, to enable communicable models of practice to take hold and for real-world network functions to develop to begin to take advantage of systems (i.e. AI-tools, decision support systems).

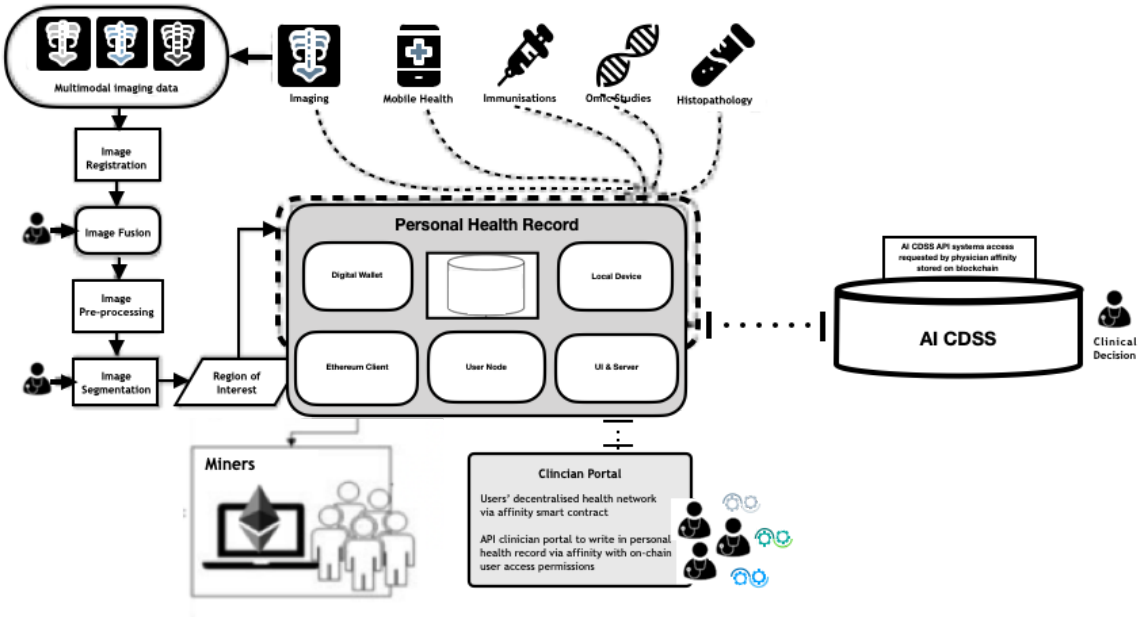
7. Health Systems (Intelligence Layer)

Doctelligence defines health systems as those which store, retrieve, generate, send, and process health data in the provision of healthcare (e.g. clinical decision systems, diagnostic algorithms). They are central role-based entities and important to the decentralization of healthcare ecosystems and the network separates out their functions to facilitate physician-user steered provision within the network as part of a learning health system [6].

The network enables systems to interact with participants (i.e. physicians) using sovereign identities with public/private key pairs to embed intelligence into provision. In particular, the network focuses on the implementation of artificial intelligence-clinical decision support systems (AI-CDSS) that underpins a central meshwork in the development of new models of health care practice. There are other AI- systems/tools which use comparatively simple inputs to achieve certain thresholds of accuracy and quality health information (i.e. automated mobile EKG diagnosis, medical imaging diagnosis etc). Such tools drive a single output, however, and are useful in that they can improve the accuracy of the steered course of provision in health care pathways (i.e. reduce time). It is also important to distinguish data-inputs and outputs of systems technologies whereby the former utilises health data inputs to develop their inherent value (i.e. Mobile EKG device). The outputs need synthesising to inform clinical decisions at key points in clinical care pathways and form the centre-piece of clinical healthcare provision. AI-Clinical Decision systems invest in physician-machine partnerships to deliver AI-based healthcare at crucial points to users in clinical care pathways. This is achieved by drawing on fundamental principles of AI-physician interactions, user-physician interactions and inference (i.e. White-Box AI-algorithms).



A model of health provision is considered as the implementation of decision support systems into clinical care pathways (i.e. triage, diagnosis, treatment, prognosis) fed by other supportive systems (i.e. omics, mobile health, imaging). Health systems typically rent out their software via web-based (cross-platform) solutions with supporting applications and integrate into the network using their public/private key pairs to access API-portal gateways to personal health records using permissions associated with their own sovereign blockchain identities; systems attach in a similar way (i.e. cryptographic access tokens) to joining physician (or other roles) of a health care practice to access personal health records of the user in the provision of healthcare. On-chain metadata can specify for user-system, and system-provider affinities which grant access to users' personal health records to facilitate healthcare provision. Systems (i.e. clinical decision support systems) can similarly use their identities to make use of the authentication architectures held on *authentication* smart contracts to validate licensing (i.e. FDA/CE) in the appropriate jurisdiction and when required to do so; though many open-source health systems may not need to do this. Health professionals steer provision (i.e. healthcare) with users and are responsible for informed and shared-decision making, as well as expenditure, in healthcare [1]. The architecture enables user-physician relationships to mediate the direct purchase and control of systems technologies and to fulfill the potential of the sovereign setup of healthcare [1]. The recording of personal health information into a users personal health record (i.e. NOSH healthcare systems), overall, enables more advanced provision and is best to support user-physician interactions in the delivery of healthcare. Health professionals now become the proprietors of constructing new creative models of healthcare practice which are more readily adaptable, updateable, scalable and competitive.



Health systems companies (i.e. AI startups) are seeking health data to develop their models, and users/providers for adoption and implementation. In centralised institutions of healthcare practice, access to one is interdependent with the other, whereby system companies regularly compete for institutional credibility to overcome a limited provider pool. These institutional providers rely on the scale of practice with care pathways that saturate quickly, limiting the adoption of new technologies, and thus, system's companies get caught in competitive dead-ends. Large-scale medical technology companies maintain their long-established partnerships with highly credible institutions and take advantage of access to and exchanges of large central repositories of health data. These repositories are often held in a cross-silo health networks of partnering institutions as strategic maneuvers to preserve data ownership.

This setup does not favour the smaller player (i.e. AI-startups) seeking access to health data to train their algorithm models on, and to enter their systems into health care practices in an already limited provider pool. The small to medium size systems companies which are successful alter their business models to develop as institutions themselves, recognising the lack of small to medium sized diverse practices who might have adopted their systems into their care pathways. And so, they begin recruiting a physician-base to integrate their systems into care pathways acting as institutions themselves; this business model quickly reaches a saturation point with a reliance on sustaining a saturated physician-base. As a result, clinical care pathways are stifled, ingenuitive practice remains obsolete, and the market remains relatively impenetrable to new system-integrated health care practices which does not benefit the individual user (i.e. patient).

Systems companies (i.e. AI startups) are provided entrance to federated learning (FL) protocols distributed on the blockchain to train their models on users' personal health records in the network, using their own sovereign public key dentities [8]. A blockchain based FL framework saves on operational costs (i.e. cloud based setup/operation) and lowers the entry barrier for smaller players and improves accessibility significantly [9, 10] whilst alying to a new pool of providers in a decentralised intelligence health network in which to market their systems to health care practice. The nature of FL is particularly well suited to handling heterogeneous data in the development of AI-clinical decision support systems. There are other avenues in utilizing health data to develop health systems which are not deterred (i.e. researchers, academic partnerships; spin outs etc). The network focuses overall on the elements which work well in developing systems integration into a learning health ecosystem of decentralised healthcare.

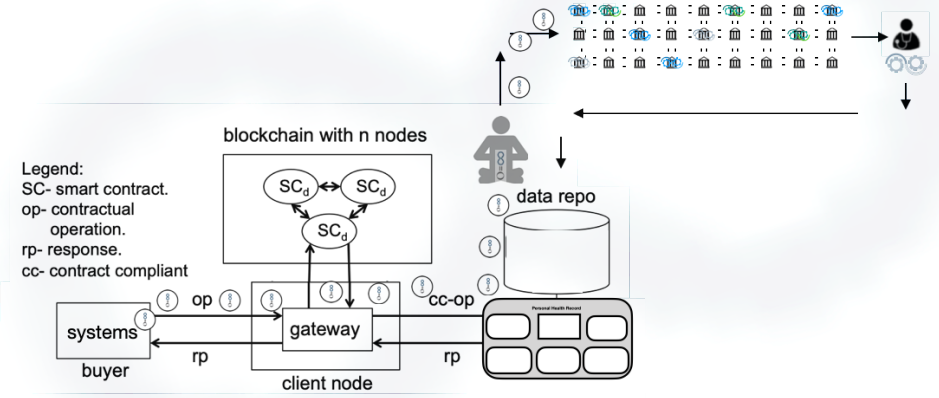
8. Federated Learning (Intelligence Layer)

The network structures access to federated learning protocols distributed across an ethereum public blockchain ledger for systems (i.e. AI-Startup companies) to train models on users' personal health records. This brings about intelligence into a decentralised health network. A federated learning (FL) protocol distributed on-chain propagates gate-ways for algorithmic models to train on users' personal health records whilst security and privacy remain innate in the network. Systems, or else, any entity seeking to train their models on users' personal health records utilises a *federatedlearning* smart contract which interacts with a *transactions* smart contact based on ERC-20 token exchanges.

Users store permissions on the ethereum blockchain to opt-in to distributed *federatedlearning* smart contracts holding protocols relevant to their personal health records to participate in a federated learning round. A *transactions* smart contract interacts with a *federatedlearning* smart contract to pre-specify the participation level of a round based on specific measures (i.e. node number, epoch, data size, inherent value, data uniformity) and local nodes bid their models to update global models [9, 10]. User-based on-chain smart contract policies detail personal health record access permissions that preserve data ownership, data transparency and audibility, as well as fine grained access control in a non-temperable way [4]. This maintains visibility and access with a pathway to developing secure access solutions for the purposes of provision and FL protocols enacted on personal health records. Fine grained access is better specified on chain to preserve decentralisation and this control maximises transparency and paves the way toward a more complete method of FL to facilitate the tokenization of health data [4].

A Participation Level (PL) is chosen for every FL learning task which specifies the number of agents which must have submitted their bids in order for a round to start, set by information retrieved from the interacting *transactions* smart contract. Once the PL criteria is met, the round begins and no new devices are allowed to participate [10]. Devices

upload their models on whom their bids were accepted and proceed to signal a close of their round as the transaction is divided amongst participants (i.e. users) in the round according to their contribution defined by the on-chain *federatedlearning* smart contract policies [10]. The community will explore the development of logical distance measures of uniformity to handle heterogeneous data, and semi-supervised federated machine learning techniques, to enable systems to make use of more specific use cases of PHR data, as well as other relevant computational techniques which optimize the FL process with a focus on optimizing protocols for the development of AI-CDSS. An option of the transaction itself will be confidential and/or anonymised though the parties who are transacting. Zether smart contracts may be extended to be anonymous (identities of transactors are private) as well as confidential [11].



A confidential payments architecture (i.e. Zether) incorporates confidential account-based (i.e. ethereum) transactions suitable to leveraging the public ethereum blockchain. It implements a private value tracking system, in which account balances are encrypted during transactions [11]. A Zether Smart Contract (ZSC) attaches to deployed ERC-20 smart contracts; once deployed this contract establishes complimentary "Zether" based accounts into which participants in the network are able to deposit and withdraw ERC-20 funds [11]. Having credited funds to a Zether account, the owner may privately send these funds to other Zether accounts confidentially (transferred amounts are private) before decrypting them into their original token-form [11]. The transaction is then decrypted and returned from the Zether account into users' digital wallets as the original token-structure. This enables all transactions which would occur over a decentralised intelligence health network to happen confidentially and/or anonymously (if required).

9. Cryptographic Insurance Solution

The tokens are deposited into users' digital wallets who were successful in bidding their model updates to a federated learning round. Users then contribute these tokens toward the purchase of cryptographic-based insurance premiums to fund their provision of health care. This mechanism enables transition into a learning health system as the insurance purchase enabled with tokens increases access to provision which in turn re-supplies health data on a needs basis into users' personal health records. Thus, users, providers and systems remain incentivised by one another to conduct their activities within the decentralised intelligence health network in the provision of and purchased access to personal health data; noting that the entity of space remains separate from the data economy.

A provider is reimbursed into their accounts associated with their public/private key pair identities by insurance companies via fiat/cryptocurrencies into the providers bank/wallets. An automated verification of health care insurance claims is handled better on the blockchain as it provides a reliable source of information with which to verify information and insurance credentials. Existing insurance providers may wish to upgrade their systems to receive cryptographic currencies to include enterprise grade mechanisms of exchange. Co-insurance, deductibles or copays can be billed to the user off-chain and this can be developed over time. It may take time for the token value to stabilise enough for it to reliably provide value and is an interdependent building block of the network.

10. Decentralised Intelligence Health-System (Root Layer, Real-World Layer, Intelligence Layer)

A model-view-controller setup distinguishes the role of the network to on-chain smart contract protocols which interact with servers and user interface applications across distributed health care marketplaces. A decentralised intelligence health network starts with the underlying assumption of users as owners of their own personal health data acting as agents in creating their own decentralised network of providers; rather than joining existing centralised health networks (though this is still possible). Health data holding shifts to a user-centric holding of personal health data with on-chain permissions determining access via an API portal [1, 2] to personal health records held on users' local devices (e.g. laptop, mobile). User-centric provision is facilitated in the real world by the selection of decentralised provision into a distributed layer of space nodes using public/private key-pair interaction and request-based mechanisms of sovereign nature. Future discussion around how the network will preserve decentralised health networks to protect the network from the re-centralisation of provision is considered.

Relinquishing institutional access as combined holders and controllers of personal health information (PHI) [1] in addition to health space completes a dissolution of the institutional entities. A decentralised health network facilitates new practices and revitalises the provider pool with new opportunities for health systems seeking practices to embed and implement their software. The architecture and components of the network do not require IT purchasing power that previously favoured large hospitals and electronic health record vendors. The dissociated capital costs are spread across a distributed layer of entities which affords systems at scale. The combination of personal health records and space nodes in real world considerations enables maximum interoperability at scale. Overall, the network vastly improves communication efficiency in the provision of care and in the utilisation of cross-device health data federated learning protocols to switch focus to a network of data access, rather than data exchanges. The latter of which are found in cross-silo architectures that lead back toward centralised provision.

The agency in the selection of space nodes enables user/community-based selections of decentralised health care provision that is more readily accessible; in turn individual, small and medium sized practices grow across distributed health space, supported through scalable models of practice afforded by emerging health systems technologies. Healthcare professionals become the creative proprietors of engineered models of clinical care pathways integrating new systems to develop market competitiveness and niche practice. Practice buy-in and the hosting of expanding models of healthcare practice are marketplace considerations and present new opportunities for financial models of expansion which do not focus on income. The request mechanisms using public/private key cryptography prompt the delivery of models to a desired space, which lowers the capital risks for individual, small and medium sized practices, previously associated with attempting to locate to new regions. Health space (i.e. node) is a niche potential and relatively unsaturated environment for servers and applications (i.e. user interfaces) utilising the network to scale and develop their business models into distributed marketplaces [14]. Individuals or communities encourage diversification through requests to nearby space cross-regionally, culturally and cross-border. The network encourages distributed health space marketplaces for providers to test the network with their models across different locations and populations using smaller slots of time (i.e. by the hour, day, week, month). Distributed marketplaces are in a better position to enable a health network to develop in diverse and tailored ways as differences in localities and nuances of culture, time and place, are enhanced [14].

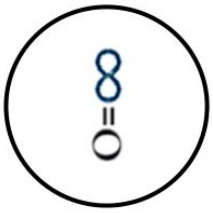
A personal health records system (i.e NOSH) designs clinician portals with basic cryptographic accesses, with the potential to maintain policies of convenience (i.e. research, audit). When all of the patient data is in a single database (i.e. PHR), a model of clinical decision support is better coordinated and works well [7]. Systems integration centres around AI-CDSS embedding into clinical care pathways in physician-system partnerships.. Scaffolding customisable

clinical healthcare pathways to structure the implementation and embedding of such tools reflects the aims of the network to enable system integration with care delivery into new models of healthcare provision. Access for systems wishing to join the network may be provided by distributed marketplaces. API time-based transaction smart contracts providing access to the API's systems utilities to users' personal health records in which providers implement them into scaffolds of healthcare provision (or else off-chain) is a roadmap of the foundation's work; cryptocurrency-based transactions are considered for all entities. A provider's server and user interfaces can structure scaffolds for physicians to develop practice models to implement system driven care pathways with components that may more readily implement semi-automated (or automated) aspects of healthcare which are more cost-effective, time-efficient, deliverable and hostable to enable time for physician decision making and user-physician interactions which typically define human components of delivering practice and for joining physicians to deliver based on the provider practice construct (i.e. models of practice).

The root and real world layers of the network remain incentivised to scale independently as core mechanisms of real world develop a decentralised health network whilst the intelligence layer is interdependent and can develop and scale steadily. This enables the community to focus on developing on-chain federated learning protocols over time and to introduce such protocols at a point in which they sustain a surplus in value exchange for users. Consensus in the community can be sought surrounding implementation of this component of the network. A cryptographic based insurance does not rely on fiat currencies to accrue or stabilize in value, thereby supporting access to healthcare across a variety of state economies (i.e. developed, undeveloped, developing, unstable). Coupled with region-syncing authentication architectures, this enables participants in the network to add a new layer to present healthcare systems. These components form the basis to developing decentralized healthcare whilst establishing a long term roadmap to a cryptographic-insurance and subsidy in universal health coverage. The network will access distributed marketplaces (i.e. physicians, spaces, systems directories etc) supported by servers and user interface applications chosen by participants utilising their sovereign identity architectures.. Users can access their sovereign identities in distributed marketplaces using one of a community supported, commercial or sovereign based servers with complimentary user interfaces (UI) [1]. A user centric root infrastructure of self-sovereign identities centre user agency to enable an individual to act through the decentralised intelligence health network to choose their own healthcare services, healthcare providers, influence the location of healthcare provision, and create their own decentralised healthcare networks.

11. Token

Token Name: Doctelligence
Token Symbol: "o=∞"



Tokenizing healthcare data access into a trust-less ledger realises its value directly and reflects the value propositions of a decentralised intelligence healthcare network. We seek to circulate the value of health data into a learning health ecosystem to maintain the tokens relevance and cost effectiveness in the subsidy of healthcare provision. Access to federated learning protocols enable models to train on personal health records and sustain a continuous income for users that incentivises opt-in to federated learning protocols across a blockchain network to re-circulate economic value into a learning health system. A user can preserve their own data privacy yet contribute to building global models which address healthcare challenges common to the entire community of patients with similar conditions [10]. Individual, small and medium size practices participate in decentralised health networks which enable the focus on practice growth that do not acquisitie health data as institutional assets in centralised provision..

Confusing governance mechanisms pose a hazy relationship between data privacy (i.e. GDPR) and individuals across different federated states, USA. This existing discrepancy significantly reduces the usefulness of health data released

under current models of centralised institutional provision that release data through secretive means that leaves the user (patient) out of the equation. Companies might need to obtain data through a number of layers of indirection instead of directly from healthcare sources, which substantially reduces the financial incentive to maintain patient data in forms such that they are directly useful (with clean and validated labels, for example); potential data uses such as technology and pharmaceutical companies might not have sufficient legal basis for obtaining and processing such data. Such use of data might negatively affect the trust between patients and the health sector before this is able to occur, due to the lack of clarity of the assumed permissions and confusion surrounding what opt-out actually means. These elements hinder the use of patient data for good and positive impacts in the long run which is why a token mechanism attributed to federated learning protocols distributed on-chain are a foreseeable path forward.

The network tokens are exchanged into digital wallets, transferable to other wallets, and can be used to fund healthcare provision using cryptocurrency based insurance solutions which develop over time. A learning health system ensures the return of value into the system in the cumulative development of better systems and practice, accruing token value and economies of scale whilst each participant remains incentivised by one another. A long term roadmap scales a reduction in the costs of healthcare insurance, lowering the entry barrier thresholds of access to healthcare for populations. Token issuance will analyze token sale models and seek to implement safety token sale mechanisms drawn from its initial participants and community based consensus before launch [12].

12. Ethereum Blockchain

Doctelligence chooses ethereum as its blockchain since its ecosystem is the most diverse and has the most public support and its underlying ethos aligns with the themes of the network. The foundation seeks to support these works as a centre to developing smart contracts which ensure the appropriate functions of the network.

Although legal responsibilities of maintaining ledgers in a private network based on trust exist, health providers remain competitors. A decentralised network maintains consensus via an ethereum public ledger to establish a roadmap to an entirely trustless architecture in healthcare provision all-centred on user agency. This maintains the sovereignty of participants and opportunities to continue developing a decentralised intelligence health network. This may take longer to set up network interactions of this type though it will establish societal integration and gradual momentum. It is therefore in line with the long term road map in establishing an adaptive network which enables the continuation of sovereignty.

Ethereum is an open-source blockchain platform with smart contract features that support Turing-complete operations. It can thus be used for a wide (and open-ended) set of capabilities relevant for healthcare applications in the network, including health data access control. The network handles algorithm model distribution and access to sensitive patient information, as well as facilitates communications amongst various entities; therefore an underlying blockchain platform that supports Turing-complete operations and enables programming features capable of solving any computation problem is selected.

In this model, transactions require Ether, a network currency unit, to be processed by the network. Ether can be earned by mining, awarding an acceptable amount of it to a node that solves the computational puzzle [13]. Health participants are incentivised to participate in staking as well as the decentralised intelligence health networks reward mechanism in order to fund the continuation of their activities which they can do with their personal devices in Ethereum 2.0.

13. Smart Contracts

Affinity.sol User (patient), custodians (i.e. parents/spouse/carers), providers, space node, systems, any participant. Affinity represents a relationship between entities (i.e. user-provider). This contract also manages the cryptographic token-based permissions access to data stored on the user's personal health records.

Authentication.sol Enables the signed verification of entities (i.e. physicians/providers) credentials using their self-sovereign blockchain identity (i.e. public/private key pair).

Intelligence.sol: Distributed federated learning protocols which host global models for systems to to train algorithms on users' personal health records.

Networks.sol: Associated on-chain data which summarises a user's affinity to enable their decentralised networks to live on-chain.

Transaction.sol: Time-based (epoch, batch size, data valuation etc). A transactions smart contract which values federated learning access to users' personal health records to conduct training of algorithms.

Token.sol ERC20-Token (o=∞: doctelligence token, interface)

Zether.sol Zether-anonymous protocol for token exchanges to enable confidential and/or anonymous transaction amounts of tokens.

14. Doctelligence Wallet

- Key wallets [3]
- Physical medical ID cards embedding private keys [3]

Providing an open marketplace for technologies with access to data feeds back into the network with new devices and systems and so it feeds itself which in turn gives access to more efficient models. Users transact access to train models on their personal health record rather than exchanging the data itself, with their permissions. A Zether account is set up in the doctelligence wallet to enable confidential transactions. This enables the users (patients) to receive confidential transactions from providers in ERC-20 token standards with which to deposit in their accounts.

- **Ethereum Transactions**

Decentralised application solutions implement on-chain component (smart contract) and an off-chain component (e.g. web or mobile interfaces/applications). While the on-chain code can only transact in ETH, the off-chain component is free to transact in any currency each solution requires. However, a key capability offered by blockchains is their support for "trustless" transactions between parties who lack trust relationships established between themselves [3]. Blockchains are peer-to-peer by nature and thus contribute to the ubiquitousness of digital assets being transacted whilst enabling integration with distributed marketplaces [14].

The important aspects which doctelligence seeks to supply are for developers to take advantage of distributed marketplace ecosystems which form the main integration of the network. A separate entity may wish to bridge these key milestones in integration which are enterprise focused and in which real world provision is integrated into distributed marketplaces. The entities of the system are designed to enable the potential of Ether and EIP20 tokens time-based transactions to suit each main entity in the exchanges and interactions of value i.e. space, systems, and data access which lead to provision.

15. Doctelligence Foundation

The Doctelligence Foundation (DF) works to promote a decentralised intelligence health network to mechanise upgraded models of accessible and affordable healthcare.

DF designs a decentralised intelligence health network that adds a new layer to present day healthcare systems. Collaboration with different participants will seek to set up network access through servers and user interfaces taking the experience of working with different participants in the first phase to scale real world provision and adapting to the growing scale of a network to switch on federated learning protocols in the second phase. The community will aim to provide smart contract permissioning tools, on-chain protocols and guide basic user interfaces and servers to engage users, spaces, providers, and systems to develop network integration across distributed marketplaces.

DF is a non-profit organisation dedicated to supporting doctelligence, related technologies and entities providing care. Our team comprises people from technology, medical and law backgrounds, with experience and understanding of current medical systems, advised by experts and academics from related areas. No one owns doctelligence and so

everyone owns doctelligence. It is an architecture run on the public ethereum blockchain and this means the network is not as vulnerable to attacks as there is no centralised provider and so there is not anything to take it down.

DF is not a company, nor a traditional non-profit. Their role is not to control or lead doctelligence, nor are they the only organisation that funds critical development of doctelligence related technologies. This should be made open source so people can see what the foundation is working on, as well as the foundation so that it can be critiqued. The DF is one part of a much larger ecosystem.

Conclusions

The purpose of doctelligence is to orient care into engineered pathways which build effective solutions into health systems. The old adage of medicine as an art reflects the inadequacies of present day tools to engineer heal provision [15].

Paradoxically, our ethos seeks a basis whereby individuals may realise themselves as life-oriented beings. The art must be re-found through the individuals' lived experience, through inclusiveness, spirituality, and the existential experience that is life.

References and Further Reading

1. HIE of One:
http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/7-29-poweringthephysician-patientrelationshipwithblockchainhealthit.pdf
2. NOSH Open Source Personal Health Record System: https://github.com/shihjay2/nosh2
3. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Comput Struct Biotechnol J. 2018 Jul 29;16:267–78.
4. Zyskind G, Nathan O, Pentland A 'Sandy'. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In: 19.15 IEEE Security and Privacy Workshops. 2015. p. 180–4.
5. Cities and the Balance of Power on physical space:
https://www.city-journal.org/urban-politics-shape-national-politics
6. Decentralising and separating out different functions of an ecosystem:
https://vitalik.ca/general/2020/09/11/coordination.html
7.Goldberg, H.: A highly scalable, interoperable clinical decision support service. Journal of the American Medical Informatics Association, 21(E1), 2014.
8. McMahan, H. et al. "Communication-Efficient Learning of Deep Networks from Decentralized Data." *AISTATS* (2017).
9. Ma, Chuan et al. "When Federated Learning Meets Blockchain: A New Distributed Learning Paradigm." *ArXiv* abs/2009.09338 (2020): n. pag.
10. Ramanan, P. et al. "BAFFLE : Blockchain Based Aggregator Free Federated Learning." *2020 IEEE International Conference on Blockchain (Blockchain)* (2020): 72-81.
11. Bünz B, Agrawal S, Zamani M, Boneh D. Zether: Towards Privacy in a Smart Contract World. In: Bonneau J, Heninger N, editors. Financial Cryptography and Data Security [Internet]. Cham: Springer International Publishing; 2020 [cited 2020 Sep 16]. p. 423–43.
12. Safe token sale mechanisms: https://medium.com/@Vlad_Zamfir/a-safe-token-sale-mechanism-8d73c430ddd1
13. Ethereum White Paper: https://whitepaper.io/document/5/ethereum-whitepaper
14. Kabi OR, Franqueira VNL. Blockchain-Based Distributed Marketplace. In: Abramowicz W, Paschke A, editors. Business Information Systems Workshops [Internet]. Cham: Springer International Publishing; 2019 [cited 2020 Sep 8]. p. 197â€“210. (Lecture Notes in Business Information Processing; vol. 339). Available from: http://link.springer.com/10.1007/978-3-030-04849-5_17
15. Nick Bostrom on engineering healthcare https://www.nickbostrom.com/fable/dragon.html