# Medwish : decentralized Health ecosystem

Reference version : french 2.1.6 (pre-print)

contact@medwish.io

DEC 2020

**Abstract**

A system that would allow the valorization of health data would optimise access to care.

Patient-controlled management of health data provides part of the solution to this valorization, but the benefits of this control are lost as soon as it is possible to break with medical confidentiality.

We offer a decentralised and secure health data management solution which, combined with more confidential exchanges of values, makes it possible to guarantee medical confidentiality.

The data is anonymized and encrypted individually on the client side. The data is then sent on a decentralised and secure storage network. The network is made up of nodes that manage the storage and validate value exchanges (transactions). Data access (read and write) is controlled by the patients. Patients may or may not monetize this access. Monetization or any other exchange of value over the network is carried out on a bitcoin side timestamp server of which the transactions, confidential by default, are validated by the network nodes.

We offer a solution that provides an incentive to redirect the value of health data to funding. of care, thus ensuring better access to care.

The value of health data, supported by collateralisation, is stabilised for the players in the health sector. care (patients and professionals).
Incentives to finance care are put in place, such as a moderate monetary meltdown which intervenes if the care actors do not carry out any action during a given period of time. There are two types of action, spending for immediate care or placements. There are two investments, those for future care expenses (interest-bearing) and those in the companies providing care products or services on the network.

Finally we propose a community governance with liquid democracy and quadratic voting.

In order to become a node of the network, two conditions must be met, passing a differentiating test humans from the robots and the cryptomonic sequestration on a multi-signature address managed by the governance. Participation in governance is through a second receiver. The end of receiverships is decided by the participant. The outgoing value, depends on the safety work, storage and involvement in governance.

# 1 Introduction

Life expectancy is increasing but health expectancy has tended to stagnate over the last 10 years [1]. This growing gap reflects an increase in the need for care beyond the age of healthy life expectancy and an increase in the costs associated with care (becoming unbearable by 2050) [2]). The expected decline in the number of doctors in the world's population [3] mechanically creates a decrease in access to care, regardless of age, due to a lack of health professionals and/or a lack of capacity to finance care.

We know that technological advances in medical devices or medical algorithms are significantly improving the quality of care. These advances are made possible in particular by the collection of health data. However, this collection remains entirely the responsibility of the patients who finance their creation, storage, use and results. If improving the quality of care depends on health data and if the collection of health data depends on the financing of patients then health data have a significant financial value for improving the quality of care.

We know that medical confidentiality is an integral part of the right to respect and protection of privacy, a right enshrined in the United Nations Universal Declaration of Human Rights [4]. We know that medical confidentiality cannot be disclosed without consent. However, while medical confidentiality includes all interactions with a health professional, the knowledge by a third party of a payment to a physician breaks medical confidentiality. As a result, transaction data for care purposes must be processed with as much caution as health data. They must therefore be subject to medical secrecy and no trusted third party must be able to identify a patient or the pathologies of which he is suffering without consent.

If it is agreed that the quality of care and the need for care are increasing and that medical demographics are decreasing, then the levers of accessibility to care are the increase in the population of carers and or the increase in the capacity to nuance care per individual.However, training more health professionals requires human and financial resources that are too great in the short term. Resources that we do not have.

We therefore conclude here that the best lever for access to care is to increase the financial capacities of each individual. And since we know that health data has value, then access to care must be able to be financed by access to health data.

Such an economic health policy must present, within the framework of a social consensus, measures to improve access to health care. So as to provide an incentive to redirect revenues from access to health data to access to care.

However, we know that from a psychological point of view, financial incentives are powerful in changing behaviour. Currently, the only incentives offered are through insurance health.But they are still a wasted investment for patients until the need for care is present.It would be more profitable for patients if their investment in health became a capital asset. available and remunerative as long as the need for care is not present.

If health insurers currently dictate the rules for the use of a patient's funds, issuing a new model of health insurance supposes a new decision-making model. We know that scientific experiments that study humans in a power situation all conclude that there is a need for power sharing [5].The translation of these experiments is that if the interest is the common good, then it is necessary to protect oneself from a centralisation of power by sharing it.

**In this white paper we propose a solution to the problem of access to care in the form of a decentralised, community-based health ecosystem. The ecosystem allows the use of health data while preserving medical confidentiality, and encourages the use of this value for the financing of care.**

## 2 Health data

Everything starts with the definition of a health data.

It has been established that health data are immaterial extensions of the human body, they are an integral part of what defines an individual in terms of physical or mental health, past, present or future. They may be of a personal nature if they relate to a natural person or if they present a direct link to a natural person.If no information leading to the identification of a natural person is present then the health data is said to be anonymous and if a link can be established it is said to be pseudonymous.

We are aware that some health data do not allow for anonymisation. Indeed, an X-ray and the result of an arterial tension test are both health data, but one allows anonymisation while the other does not. In the case of arterial pressure, it is presented as a two-digit result (systolic pressure + diastolic pressure) which must be linked to a patient, one day, one hour, one state of health. For example, anonymisation could consist of removing the patient's identity. The result could be written in a key/value form such as SysAt = 12 DiaAt = 8. Therefore, without linking this data to a patient, it is not possible to identify a patient other than by cross-referencing data. This would technically only take a few seconds by comparing points with a database of non-anonymised photographs.

The need is to set up different procedures for the preservation of natural persons depending on the level of initial anonymisation of the data.

In addition, we know that health data is an extension of oneself. However, if research work on health data generates new health-related data, then any data resulting from the processing of health data is also an extension of oneself. We consider all data resulting from the processing of health data to be health data relating to a patient or group of patients.

**At this stage, the problem of the notion of ownership of health data arises.**

# 3 Ownership right of health data

The right to own property is a fundamental right enshrined, and adopted by the Member States of the United Nations, in the Universal Declaration of Human Rights [4].

The ownership right is defined by the right to enjoy and dispose of a thing in the most absolute manner, regardless of the mode of legal acquisition of this right. A property right applied to personal health data would be come down to having the ability to sell, rent or even destroy it. It should be noted that in the case of health data that are not of a personal nature, a right of ownership may be established irrespective of the method of legal acquisition of this right of ownership.

Then, we can ask ourselves the following question :
Are we, as a physical person (patient), the owner of our body and by extension of our health data ?

In any case, the courts agree that the right of ownership is not opposable to the human body and by extension is not opposable to health data. Outside Iran, it is not possible to monetize all or part of our own body. Nevertheless, everyone has a right of use. This right is composed of the usus (right to use, control) and the fructus (right to profits). In other words, a patient has the right to use and control the use of his or her health data for his or her own benefit.

**We know that health data has a market value. But can the value of an individual's health data be redirected to the patient ?**

# 4 Valuation of health data

We have seen that no patient in a ONU signatory country can sell his or her health data or even destroy it. However, it is legal for a third party to trade health data if, and only if, the data is anonymised (the legal conformity of the data collection depends on the information given to the patient and the patient's consent). Health data that are not of a personal nature, nor direct or indirect links, are in fact marketable.

According to this state of affairs, a patient cannot benefit from the monetization of his personal health data, whereas a third party can. But a patient is given this possibility if and only if no link can be established between the data and his or her person.

The need could be to allow patients to regain the value of their health data in an environment that ensures that they are not connected to themselves. But all so-called pseudonymous data, such as the results of medical imaging or genomic data, would be excluded.

However, there are ways in which a patient is compensated for the use of their body and, by extension, his or her health data. In fact, at the international level, the possibility of carrying out medical research leading to the remuneration of patients has been established. This remuneration comes as compensation for participation in medical research. There are different types of research (interventional or non-interventional) but whatever the type of research carried out, the goal is the development of biological or medical knowledge following the obtaining of new health data.

It is therefore concluded that if the purpose of the treatment is for the benefit of medical research, then a patient may perceive a benefit from the use of his or her health data.

The need is therefore to enable patients to receive compensation for the use of their health data in an environment that ensures that they are not linked to themselves and dedicated to medical research, regardless of the level of anonymity of the data.

**For a third party, the absence of a link between health data and a patient results in the existence of medical confidentiality.**

# 5 Medical confidentiality

Medical confidentiality is a fundamental right of the patient and one of the pillars of medicine. It represents all the information entrusted, seen, heard, understood or interpreted during the practice of a health professional concerning a patient.

Medical confidentiality begins from the first interaction that can lead to treatment. For example, an appointment booking, whether online or offline, must guarantee the confidentiality of the information transmitted from patient to practitioner from end to end, otherwise medical confidentiality is broken.

Health data is, in fact, subject to medical secrecy, therefore any processing of such data beyond the control of the patient or the health professional (carried out by a third party) is in breach with medical confidentiality.

**There is therefore a need to set up a health data management system without a trusted third party that guarantees medical confidentiality.**

# 6 Health data management

## 6.1 Storage structure

We offer a network consisting of nodes connected to each other, forming a decentralized storage network. In the context of data management, network nodes are physical structures for hosting decentralized databases.

Decentralized storage makes it possible to go beyond the limits of centralized storage. It provides more reliable storage that is more accessible, more scalable and more resistant to certain types of attacks, such as denial of service (DDOS).

## 6.2 Anonymisation et pseudonymisation

Before being stored on the network, each piece of data must undergo a process preventing direct or indirect re-identification of individuals (anonymisation) or, failing that, a process preventing direct re-identification (pseudonymisation).

However, the process put in place should not be a hindrance to medical research. For example, deletion of the patient's first and last name is obvious, but the date of birth is often fully removed. Indeed, although it is easy to re-identify centenarian patients, replacing a date of birth by an age bracket makes it possible to mobilize data sets that were previously unavailable for research, while preserving a high level of anonymisation or pseudonymisation using high-performance data.

With a view to preserving medical confidentiality, we propose that this treatment, which is the first step in data management, be carried out on the client's side.

**However, anonymisation or pseudonymisation is not sufficient to guarantee data security.**

## 6.3 Encryption

Encryption is a cryptographic process whereby data is made unreadable by a person who does not possess the decryption key.

In the context of medical confidentiality and its preservation, as well as in the context of the re-appropriation of health data by patients, the choice of the type of encryption becomes an issue. The encryption to be applied depends directly on the type of health data. It must allow health data to be kept as static as possible (i.e. allow as little movement of health data from one place to another as possible).

Moreover, it seems important to encrypt data with unique keys in order to reduce the profitability of a brute force attack (a brute force attack is a principle of cryptographic analysis consisting in testing all the possibilities of decryption keys). Indeed, if a set of several data (dataset) of significant value is encrypted with the same encryption key, then the profitability of a brute force attack may be in the attacker's favour.

Homomorphic encryption provides part of the solution but its effectiveness is greatly diminished for medical research if data has not been encrypted with the same encryption key. Indeed, the purpose of homomorphic encryption is to allow calculations to be performed on encrypted data (through the encryption layer) without having access to unencrypted data. Homomorphic encryption presents itself as one of the best alternatives for static, patient-controlled data and for outsourcing calculations. But as soon as a calculation is made on data provided by several patients, each with a different encryption key, then the complexity is such that the benefit of homomorphic encryption is lost.

A branch of cryptography is interested in secure multiparty computing (MPC) [6]. The objective is to design solutions that allow several parties to calculate together a function of their data, while keeping this data secret. Contrary to classical cryptography, where one seeks to ensure security despite the presence of an external adversary, the MPC guarantees security against an internal adversary controlling one or more participants. Taking advantage of the MPC would make it possible to become more respectful of privacy.

However, allowing the realization of a function *f(x)* reveals some $x$ and if there is no other additional security, one gives in theory the possibility to discover the data $x$.

We propose the implementation of the MPC system associated with unitary data encryption and the addition of noise. This means that each piece of data has a different decryption key and is only accessible to the patient. Noise, on the other hand, is defined as the addition of data whose value is taken randomly in the interval constituting the known standard. These data have an insignificant impact on the final result. The unitary encryption associated with noise would make an attack not profitable. Finally, this encryption system allows the data to remain static and total control by the patient

This raises the problem of decryption. If encryption is an issue, it is also necessary to consider decryption. For example, homomorphic encryption poses the problem of computing power and therefore the time needed to perform calculations through the encryption layer. However, the amount of computing power that can be used today in conjunction with Moore's Law [7] makes it possible to minimize this problem. Moreover, if we take into consideration the fact that the profitability of mining cryptocurrency is becoming increasingly low for private individuals, it would be profitable for everyone to allow this computing power to be allocated to medical research needs based on encrypted data in the same way as the computing power allocated to protein folding [8].

We have proposed a solution to encryption. The anonymised and encrypted data is then sent over the network and duplicated on random nodes, so as to maintain three copies of it at all times for accessibility purposes.

**The issue of data control and access now arises.**

## 6.4 Control and access to data

If only patients have the right to use their health data, then they should be the manager of health data access rights.

We propose that the control of access rights to read and write data should be controlled by patients or any other person defined by the patient himself (an assignee, governance of the network for a limited period of time, others). The patient holds the private keys of this access manager and these private keys are transferable after encryption to a trusted third party chosen by the patient. Exchanges are carried out on a purely peer-to-peer basis. The patient can change the access rights at any time. He can therefore authorize read access to his data or even request the total deletion of his data from the network (after having downloaded them).

In addition, access rights to storage facilities are non-automatically controlled, i.e. voluntary action on the part of the patient is required.

**Controlling the data does not define how the data will be shared.**

## 6.5 Data Sharing

Between care providers, no limitation is to be expected. The health data necessary for the proper treatment of the patient are at the discretion of the patient and his or her health care professional.

In the context of a request for access to data made by a third party, in particular for medical research, it is necessary to limit the number of treatable data per patient resolving the problem of re-identification [9].

## 6.6 Use case

A third party, in the framework of medical research and in a public way, identifies himself, states the purpose of data processing in a clear and intelligible way, specifies his/her search for data (inclusion and exclusion criteria in the study), publishes his research protocol and informs the patient of his rights and compensations.

This declaration of intent and data search is posted on the network on a dedicated storage space. Patients can check whether they have the capacity to meet the demand for medical research without interaction with third parties. The patient, enlightened in this way, may or may not consent to satisfy the request for access.

The identified third party requesting the network undertakes to publish the results of its work in open source, whatever the status (finalized or not) and its results (meaningful or not) on a dedicated and resilient space specific to scientific publications. In addition, they are obliged to attribute any new data created to the patients' usufruct. In the event of non-compliance with this obligation, the identified third party will be denied access to the network by the governance.

## 6.7 Technology at launch

For decentralized data management we use the tools and services offered by Protocol LAB for the creation of the IPFS [10] (InterPlanetary Files System) coupled with the solution proposed by Textile.io [11].

**However, we are aware that this structure remains incomplete to guarantee medical confidentiality and that confidentiality must be ensured for exchanges of value.**

# 7 Lateral timestamp server

Medical secrecy, which is an integral part of the right to privacy, leads us to identify a serious problem:

The current opposition to the right to privacy and increased surveillance in the context of the fight against money laundering and terrorist financing (AML/CFT).

In any case, and generally speaking in financial matters, AML/CFT is prioritized to the detriment of the right to private life.

The consideration of this state of affairs leads us to orient ourselves towards the Bitcoin protocol [12]. The latter is an electronic cash system where a coin is defined as a chain of electronic signatures. This principle makes it easy to follow the movements of the electronic parts and meets the needs of the LAB-FT. However, at the present time, the completion of a transaction on this protocol is identifying and therefore in breach of medical confidentiality if it were to be carried out as a regulation of care. Finally, it should also be taken into account that this environment remains limited in terms of the number of transactions per second.

We therefore propose the implementation of a bitcoin lateral time stamping server, commonly known as *sidechain*, in order to benefit from the resilience of its network. This installation makes it possible to solve the problem of LAB-FT by concentrating the actors of monitoring on the flows entering and leaving the side-chain.

If the incoming and outgoing flows are controlled, then exchanges within the side-chain can be more confidential.

Exchanges of public values, but more confidential and contained, values between health care actors make it possible to guarantee medical confidentiality.

For this solution we will initially use the tools and services offered by Blockstream as part of the creation of the Liquid network [13] which allows a sufficient volume of anonymous exchanges in terms of number of transactions per second.

We note that solutions such as Taproot [14] could change the vision of the security of medical secrecy on public protocols but may pose a problem at the level of the LAB-FT. If there are other time-stamping structures capable of hosting the ecosystem, the initial technological choice that we propose is based on the resilience to attacks of the Nakamoto protocol [12] and a default confidentiality via the Elements platform [15]. Finally, the possibility of deploying intelligent contracts with trustworthy results via Simplicity [16] is a reassuring asset.

**Now that the technological building blocks for meeting storage and security needs have been identified, the initial rules of social consensus need to be established.**

# 8 The Network

## 8.1 The Nodes

The nodes participate in decentralized storage and validate transactions. Transaction fees pay for the work of the nodes.

Nodes can join and leave the network at any time. To become a network node it is necessary to make a sequestration of a bitcoin value, the amount of which will be specified later. The sequestration is carried out via a multi-signature address managed by the governance.

Leaving the network is like asking for the release of the sequestration. The request for release is made to the governance of the network. The release of the sequestration takes place after the data stored on the outgoing node has been transferred to another node of the network.

## 8.2 Governance

While everyone is free to participate or not in the network, participation in governance requires proof of interest. Governance nodes are network nodes that have demonstrated an interest in governing. This evidence of interest is often materialized by a governance token. It appeared to us that the functionalities of block-chains resolve the need to create a new token without compromising the secondary interest of reselling its rights.

Secondly, the level of decentralization is an important element in the robustness of a network. It is therefore necessary to implement solutions that limit the creation of nodes per person while ensuring that the node owner is human. And if the interest is to maximize the level of decentralization, then an incentive to govern must be put in place.

Finally, governance must be able to operate through the voting of motions that are free to be tabled. Governance must be able to respond to a need for voting on motions that may be high and/or urgent. If it is in fact accepted that there are minority and majority group voters, the 1:1 vote becomes inoperative for a choice of common good. It is then necessary to allow the weighting of the vote according to its importance for each person.

We propose the implementation of a proof of sense for the nodes start-up and during the votes. Proof of sense is a test required to differentiate human users from possible malicious robots, reducing the risk of centralization and the profitability of a sybile attack. Proof of sense ensures that a human votes on motions and also ensures a level of decentralization [17].

We propose that a second sequestration is necessary to participate in the governance of the network. There are costs associated with this request and these costs will finance the development of the network. In addition to the voting right, the governance nodes benefit from an additional premium on top of the rewards for the work of storing and validating transactions. This additional premium will eventually cover the costs of participating in governance. This premium is defined as a percentage of all values that are used to pay for patient data access fees. This premium is therefore payable by any third party requesting the health data network.

We propose the implementation of quadratic voting [18], which makes it possible to defend one's convictions in the face of a majority, within the framework of a liquid democracy [19] where voting delegation is possible.

At maturity date, i.e. when the creators of the network withdraw from the governance or in a maximum of 5 years, the governance may or may not modify the modalities of proof of interest at its convenience.

**We have proposed governance, but the decentralized aspect of a health environment does not ensure the financing of access to care.**

## 9 Financing access to care

Here we are only talking about the financial capacities of the patients themselves and not of the care institutions. The latter are invited to express their interest in participating in governance.

We know that health data has a market value and is, after treatment, an important source of income for medical research, the medical device market or even artificial intelligence (AI), which is a major consumer of data.

We also know that targeted advertising is a powerful tool for businesses because it allows a better buying experience, more relevant messages, better adapted to the interests of their targets, conversions into higher sales and therefore a more valuable advertising product.

The need is therefore to redistribute equitably and without intermediaries, the compensation for access to health data and to generate additional income through the donation of patient care.

We propose that each patient should be able to freely (with consent) allow access to the processing of his or her health data and that, as far as possible, the health data should not be disclosed to third parties. Any need for access to health data, other than that of the patient, requires the payment of compensation to the patient.

We propose that advertisers operate in a similar way to medical research. Advertisers pre-publish their advertising products on a dedicated space and pay the publication costs to the governance. The publication costs include patient care, networking and governance costs. The latter then validates the publication. A patient identifies his needs and preferences on a networked application. His preferences are stored as health data. The application queries new advertising entries. If an entry matches the needs or preferences indications, the patient is notified and can view the advertisement. The patient is then rewarded by the advertiser in addition to any promotion included in the advertisement.

**Now that the means of financing have been established, it is necessary to lay down general economic principles.**

## 10 General Economic Principles

An economy structured laterally to a currency presupposes having economic principles that support that currency.

The actors of care and the network nodes do not have the same expectations and the acceptance or not of the volatility of a cryptocurrency can be a point of friction. Some predictions predict that the price of Bitcoin will stabilize after the last performance bonus is issued, around 2140. On the scale of a human life, it would not seem ethical to wait for stabilization to promote access to healthcare, whether near or far.

Then the growth in the number of stable workers shows, by their volumes of exchanges, and in any case, a cognitively ecological and reassuring aspect. Therefore, establishing relative stability from a volatile asset (compared to a so-called stable fiat asset) requires collateralization and the exclusion of any fractional reserve principle. However, the issue of a stable asset does not solve the problem of hoarding (the principle of accumulation of value outside the economic circuit) which reduces the velocity of a currency (the principle of circulation per unit of time). This velocity is an element of appreciation of economic dynamism. In terms of health, velocity could become a particularly important indicator. The greater the velocity, the more it would indicate that access to care is efficient. If we are interested in experiments to accelerate the velocity of a currency, Gesell with his principle of melting money [20] has shown that it tends to render the phenomenon of hoarding inefficient, without distinction of wealth and while increasing the velocity of the assets.

The need is therefore to obtain, only for those involved in care, a stability of the value held, anticipating the stabilization of the underlying, as well as a principle orienting the value more quickly towards care.

We propose that requests for data or promotional material be regulated at the governance level exclusively in Bitcoin. This regulation includes:

- Transaction fees to the benefit of the validator node.
- The feeding of a collateral.
- The bonuses of governance nodes.
- The financing of data access rights or patient care.

We propose that for any collateral input value, a stable value equivalent be transmitted to the patients and executed by the nodes. The stable value transmitted to a patient is dependent on the optimal geographical area (dollars, euro, etc...) defined by the patient. This stable value then follows the re-basing index of its zone [10.1]. This re-basing index is suppressed as soon as it is equal to the smallest unit of currency in that zone.

We propose the implementation of a monetary meltdown [10.2] (loss of value over time) of portfolio addresses (of care providers) which receives values from a data access compensation or from the gift of care. The meltdown feeds the collateral and governance bonuses. The melt is calculated by validators if and only if no action in favour of care is carried out within a given time frame.

Experiments also show that the interest of a melting currency exists only if the asset is liquid. And we know that, at present, the acceptance of cryptocurrency by companies offering products and services is growing less rapidly than their speculative or reserve asset interests. The need then is to promote the liquidity of the asset.

We propose that the ecosystem should equip itself with care products or services that accept this currency as soon as it is launched. The products or services put in place at the launch will, like the ecosystem, offer community governance, and will support the economy of the ecosystem while interacting with the world outside the ecosystem.

## 10.1 Re-basing

Rebasing [21]is the principle of establishing a stable value so that the value held at T0 is equivalent to the value held at T1. To do this, the system proposes a rebasing index corresponding to the average exchange rate obtained from a decentralized oracle.

The problems of indexation, the target value of the monetary unit (dollars, euros, yen, etc...) as well as the defined relining method arise.

We define the rebasing index as the average of bitcoin sales prices in the markets of the optimum geographical areas. The index is updated for each new block by validators using information from the oracles.

We define each target unit value as equal to the fiat currency unit value of the optimal currency zone concerned. For the dollar zone the unit value will be the US dollar. For the Euro zone the unit value will be the Euro, etc.

We define the method for determining the rebasing index as the ratio between the capitalisation at Tn+1 and Tn block of the side chain. If the capitalization has increased by 8% between T0 and T1 the rebasing index is 1.08. If between T1 and T2 a decrease of 3.85% has occurred, the rebasing index becomes 1.03842, etc.

The stable value has the following expression:

$$AS = SAT/IR \tag{1}$$

AS = Stable Assets,
SAT = 1 Satoshi,
IR = Rebasing Index

**The rebasing offers the desired reassuring stability, but it is advisable to invite exchanges.**

## 10.2 Monetary melting

The portfolio addresses of the care providers have an optimal stability in terms of geographical area value when a care promotion is carried out. If a portfolio is without activity over a period equivalent to a quarter, a value melt of 0.5% per week is calculated by the validator node.

We define a care action as an exchange of values between a patient and a healthcare professional or the completion of a transaction in favour of the acquisition of an immediate or future care product or service.

If we put forward the hypothesis that the value received by patients is consequent from the start of the ecosystem, the incentive produced by the monetary meltdown could produce the undesirable effect of over-consumption of care and in particular an over-consumption of medical consultations in a declining medical demography.

**If the melting of money invites the circulation of money, it is necessary to invite that the expenses are also for future care. It is therefore imperative to offer an investment in long-term care.**

## 10.3 Health investment

Health prevention is defined as the action of protecting oneself from a situation that could cause a health risk.

While banking financial systems follow the principle of fractional reserve to finance themselves, health insurances establish reserves that follow the performance of their stock market investments resulting in their exposure to the risk of systemic crisis.

Therefore the need for a patient to have the assurance of future care outside the financial markets.

On the other hand, current health insurances are limited, they remain investments at a loss for the patient as long as the need for care is not present, they do not generate any interest on the sums deposited, they are not very modular and the capital invested can hardly be carried over from one year to the next and, above all, is immobilized.

It is therefore advisable to allow this investment to generate interest as long as it is not spent, that it can be mobilised at any time, that it can be modular as desired according to the needs of care (dental, optical, etc.).

We propose that the capital invested by patients for their future care should generate interest. The interest comes from:

- Or to make its funds available for loans and insurance towards other care providers. The risk is contained by the transfer of data access control rights from the applicant to the lender as well as the orientation of the perceived values for gift of care to the lender.A process that runs until the financing granted is repaid. At maturity, the third party applicant recovers all his rights.
- Either by making funds available in collaterals for flash loans on the financial markets.

Interest rates are voted by the community on a quarterly basis. The invested capital is transferable to beneficiaries defined by the patient as long as a debt is not outstanding. At the maturity of a debt, the defined beneficiaries recover their capacity as beneficiaries.

This insurance management is allowed by smart-contracts and has the benefit of stopping the melting of the currency. In addition, it provides visibility on the demand for care products and services. This allows better anticipation of production for these suppliers.

**We have insured the exchange values, invited exchanges for the purpose of care in a health insurance operation, but the asset must be made liquid, i.e. it must be accepted in exchange for care products and services outside health professionals.**

## 10.4 Community-governed care products and services

Suppliers of care services and products are key players.

And if it is accepted that accessibility to care is everyone's responsibility, then care products and services from the ecosystem should be proposals from the ecosystem actors, for the ecosystem actors by the ecosystem actors.

We propose the setting up of services and products of care with community governance favouring access to care without limitation of evolution outside the ecosystem.

If we express accessibility to care, first and foremost in terms of services, naturally an online appointment booking service must be offered free of charge to all (patients and health professionals).

We offer the service, which is in the process of being created, under the name of **Heallers** . **Heallers** will enable online appointment booking, all e-health services such as teleconsultation and an information point for patients that can be used by institutions.

If we translate accessibility to care in terms of medical devices in daily use and not subject to certain classification constraints, it appeared to us that 7 out of 10 people wear optical equipment.

We offer the **EyeEarth** solution, currently under development. **EyeEarth** manufactures optical and solar equipment that respects the environment by recycling waste (coffee grounds, green algae, etc.).

**We therefore offer, from the start of the network, care products and services.**

# 11 Conclusion

**We have proposed a decentralized health ecosystem that solves the problem of access to care.**

First of all, we offered a decentralized and secure storage system for health data. This structure remains incomplete in order to guarantee medical secrecy. We then proposed a lateral timestamp server which offers a security of medical confidentiality. The two systems thus defined do not ensure a necessary and sufficient level of decentralization. We therefore proposed a community governance system that resolves the problem of the level of decentralization. The system thus decentralized does not ensure the financing of access to care. We have proposed a secure method of valuing anonymised data and gift of care. With the initial means of financing established, we have proposed the general economic principles defining the economy of the ecosystem. Finally, we have proposed a solution to make the exchange of values that resolves the problem of access to care liquid and for the benefit of care.

# References

[1] WHO World Health Organization. *The Global Health Observatory.* World Health Data Platform, 2020.

[2] OECD Organization for Economic Co-operation and Development. *Healthcare costs unsustainable in advanced economies without reform.* Organization for Economic Co-operation and Development, 2015.

[3] DREES Direction de la Recherche des Études de l'Évaluation et des Statistiques. *Comparaisons internationales des médecins.* Direction de la Recherche, des Études, de l'Évaluation et des Statistiques, 2017.

[4] United Nation. *Universal Declaration of Human Rights.* United Nations General Assembly resolution 217 A, 1948.

[5] Dacher Keltner. *The Power Paradox: How We Gain and Lose Influence.* Penguin Press, 2016.

[6] Yehuda Lindell. *Secure Multiparty Computation for Privacy Preserving Data Mining.* Journal of Privacy and Confidentiality, 2009.

[7] Gordon Moore. *Moore's law.* Electronics Magazine Vol. 38, No. 8, 1965.

[8] Foldingathome.org. *Foldingathome.* Foldingathome.org, 2000.

[9] Luc Rocher Julien M. Hendrickx et Yves-Alexandre de Montjoye. *Estimating the success of re-identifications in incomplete datasets using generative models.* Nat Commun 10, 3069, 2019.

[10] Juan Benet. *IPFS - Content Addressed, Versioned, P2P File System.* Protocol labs, 2014.

[11] Sutula Hagopian Gozalishvili Hill And Pick, Farmer. *A protocol event-sourced database for decentralized user-siloed data.* Textile.io, 2019.

[12] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* San Val, 2009.

[13] Blockstream Corporation. *Liquid Network.* Blockcstream Corporation, 2018.

[14] Gregory Maxwell. *Taproot: Privacy preserving switchable scripting.* Bitcoin-dev Linux Foundation, 2018.

[15] Elements community. *Elements Project blockchain platform.* Elements community, 2015.

[16] Russell O'Connor. *Simplicity: A New Language for Blockchains.* Proceedings of the 2017 Workshop on Programming Languages and Analysis for Security. ACM, New York, NY, USA, 2017.

[17] Idena Network. *flip challenge.* Idena.io, 2020.

[18] Vitalik Buterin and Glen Weyl. *Liberation Through Radical Decentralization.* medium, 2018.

[19] Alois Paulin. *Ten years of liquid democracy research an overview.* Central and Eastern European EDem and EGov Days 338 (July):455-66, 2020.

[20] Jérôme Blanc. *Silvio Gesell's theory and accelerated money experiments.* ffhalshs-00119192, 1998.

[21] Ferdinando M. Ametrano. *Hayek Money: The Cryptocurrency Price Stability Solution.* SSRN, 2014.