Blockchain - Design for Social Impact

A Work in Progress and a first draft

It is now dawning on us that the most important aspect of "blockchain" is crypto-economics alongside the possibilities for mechanism design. Borderless and trust-less peer to peer transactions, governed by smart contracts, will satisfy Coase's [1] theorem for determining the lowest cost of transactions. In this environment, in which contracts are enforced by code, traditional corporate structures will no longer be the most effective mode of organisation but displaced by a collaborative commons.

Upgrading the current banking infrastructure in favour of Distributed Ledger Technology is long overdue but is mostly only a defensive move to cut back office costs inside a closed and stagnated system. The removal of middlemen and implementation of "the permission-less model of innovation" are of more fundamental importance - but what is genuinely novel; is **the power to distribute "the creation of money" and thus resource allocation.**

It can be argued[2] that the most powerful function of the kind of FIAT money in use today is not to be a medium-of-exchange, a unit-of-account nor a store-of-value but a system-of-control. We are using this power to do good - to incentivise those with the power to achieve certain desirable outcomes!

The Collaborative Commons

All power in society emanates from the privilege of creating and distributing the medium for economic exchange - money. This has always been the domain of kings and governments and more recently delegated to banks when issuing credits.

We have already seen the emergence of open source production of software and collaborative, but legally questionable, distribution of digital content on bitTorrent surpass the enterprise in scale and quality.

These particular collaborative commons examples are sustained by the direct mutual benefits derived. In general, however, it is necessary to inject a medium of exchange and digital tokens to establish more complex value networks. In a near zero marginal cost society of abundance, value and the representation of it will not be one step removed as a social construct but It will be directly generated around the only resource that still remains scarce and non-automatable - human creativity.

---

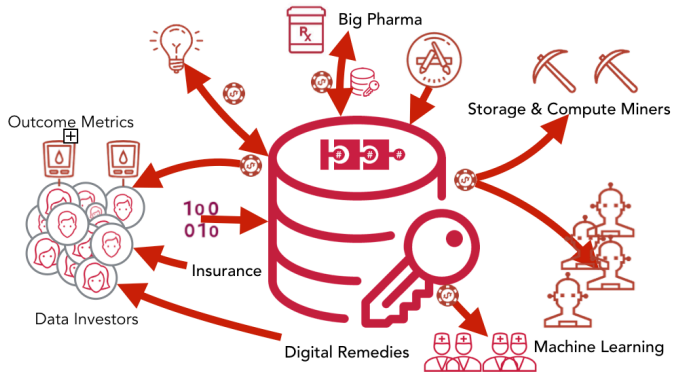
[1] https://en.wikipedia.org/wiki/Coase_theorem

[2] https://www.youtube.com/watch?v=AsbAGMPpZ6g

This is where carefully designed Smart Impact Tokens issued to incentivise exactly the desired behaviour and outcomes will; displace and outcompete the centralised capitalistic power structures.

Incumbents need to pay attention and consider their options to avoid disruption and potential obsolescence. Money will be created at the point of value creation - not at the point of control.

Proof of Concept



As a first practical example of how this can play out CareChain AB is currently , together with one of the global pharmaceutical companies, designing a concept for a *collaborative commons based insurance model* primary fuelled by personally invested health data. This is the embryo of Health-as-a-Service where subscriber data is continuously mined to optimise outcomes while predicting and reducing costly incidents. Additionally, patterns and markers will be discovered from cohort analysis to discover coping strategies and therapies. We can see the emergence of a new industry that is the fusion of insurance and pharma where the emphasis is on prevention rather than medical intervention.

In another - still stealthy - project we are applying the concept resource allocation for the immensely costly and multidisciplinary process of pharmaceutical development. Starting from unique and precision engineered epitopes from a lab process invented and patented by Swedish Researchers we are able to adequately incentivise a group of rational and autonomous actors to apply machine learning analytics and other essential skills in exchange for tokens. The researchers claim to be able to generate hundreds of protein antigen candidates - way too many to develop for any single organisation, hence the crowd intelligence approach. When it comes to the actual development of models we are inspired by the crypto hedge fund Numer.ai.[3]

Making the future come sooner

We are convinced that the best way to predict the future is to build it ourselves, hence the CareChain initiative where we are establishing the required infrastructure to realise these concept on a large scale; starting in Sweden and expanding to the rest of the EU and next the world. The lower layers of the blockchain infrastructure will eventually be self-sustained by the already tried and tested protocols rewarding the operators and validators guaranteeing the security and the integrity of the ledger (it is an impact token minted where the value is created). However, a substantial effort will be needed, not to develop the technology, but to orchestrate

[3] https://medium.com/numerai/encrypted-data-for-efficient-markets-fffbe9743ba8

the key players in the ecosystem to join the consortium and establish consensus around protocols, semantic standards and network governance.

Above we outlined a few of the applications made possible by an architecture where data is addressed by identity and not by in which silo it is locked up in. In the following sections we present an overview of the foundational CareChain concept enabling Impact Tokens and specifically for Health; further rationales and our immediate roadmap.

CareChain as such is indeed an Infrastructure Impact Token.

Johan Sellström
Co-founder, CareChain AB
johan@carechain.io
+46709756404
https://www.linkedin.com/in/johansellstrom/

> *❞ When laying the foundation for a robust interoperable healthcare system, we need to start at the protocol level and design new infrastructure that is owned and controlled by no one and everyone. We need identity and digital value protocol layers and we need immutable health records controlled by their rightful owners. Due to regional data protection regulations, like GDPR, privacy sensitive information, like health records, must be guaranteed to stay within specific geographic jurisdictions. This is why public chain deployment is not yet an option.*
>
> *Together with The Enterprise Ethereum Alliance, we want to contribute to the development of required tooling and policy frameworks to run permissioned blockchains as critical infrastructure. Leveraging the decentralized computing platform, we are reinventing data management for the entire healthcare system. We are forming a consortium, CareChain, to deploy Trusted Infrastructure, starting in Sweden and the European Union ❞*
>
> **From the press release when CareChain joined the Enterprise Ethereum Alliance [4]**

CareChain is an initiative and a consortium that aims to create a national blockchain for health data. A blockchain makes it possible for the first time to give individuals ownership and control over their own health information.

It is no longer just technology enthusiasts who collect data about themselves via their own sensors (wearables). A study from 2016 [2] shows that 32 percent of the population in Sweden registers their weight and that 26 percent registered their training data. Twenty percent have shared self-generated data with care practitioners. The number of individuals engaging in their own health and care is rapidly increasing, with the technological development of wearables and sensors instrumenting the human body moving at amazing rates.

Healthcare and research professionals are showing an accelerating interest in supplementing journal and research data with large amounts of self-generated data. Such a wealth of data allows them to extract key insights by running analyses across the entire data and full history, including each measurement, journal entry, diagnosis, drug intake, surgical procedures as well as environmental and lifestyle factors that contribute to health and disease risk.

This raises the question of who actually owns the information and under what conditions others can be permitted access, and for what purposes. Here we can see an attitude shift that, in combination with new legislation such as PSD2 [] and a European Data Protection Regulation GDPR, enhances the rights of individuals to their own data.

[4] https://entethalliance.org/enterprise-ethereum-alliance-release-05-19-2017.pdf

We envision individuals themselves possessing and managing the rapidly increasing amount of health data and thus gain the opportunity to actively engage in their healthcare as consumers rather than merely as patients. Additionally, they become empowered to offer both healthcare professionals and researchers access to their entire health history as well as to directly purchase services in a global marketplace to improve their health.

To unlock this potential, a number of challenges must be addressed.

1. **A universal digital ID**. All health data must be rooted in a universal digital identity owned and controlled by the individual. It is a cornerstone in each system designed to put the individual at the center.
2. **Guaranteed, Integrated Information Integrity.** The system must in its basic structure ensure that the information is authentic and cannot be manipulated.
3. **Built-in policy guarantees with traceability**. All actors must be able to verify that sharing, analysis and other handling and use of the information has been done based on the owner's, ie the individual's intentions and in accordance with applicable laws, regulations and processes. All events must be verifiable and traceable to all actors

The Blockchain - part of the new internet

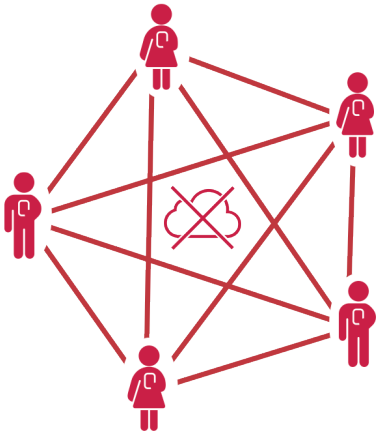
The research in cryptography and decentralized systems that allowed the crypto exchange Bitcoin has produced technology in the form of new communication protocols that enable fully decentralized systems to be built in which all actors can act based on a common definition of truth. This truth is forever enrolled in a digital ledger accessible by all actors and which cannot be manipulated. It is a common misconception that this means that posted events cannot be changed. Of course, that is not the case. The information can be updated in the same way that you can register a verification to correct an error in the bookkeeping. However, history is always left untampered.

For a crypto-currency such as Bitcoin, the ledger contains all transfers of Bitcoins (transactions) ever made on the network, so that all stakeholders can know who owns specific bitcoins and ensure they can not be used more than once.

Bitcoin has been followed by several further developments of the concept, such as the highly acclaimed Ethereum [], to support business relations and processes being run on the same integrity-assured basic technology, as well as other related protocols for decentralised messaging and data storage. Hereafter, we refer to all of these technologies as the Blockchain (or Web 3.0) in the absence of an established term. While Bitcoin's ledger handles the latest balance, ie. which identity controls what bitcoins, Ethereum generalises the concept to keep track of the state of a program, ie the current value of input and output variables. This type of program is called *Smart Contract*.

Decentralized Systems

A decentralised system consists of a number of parties acting individually to achieve the overall function of the system. The actors in a decentralised system can organise themselves, identify



each other, as well as protect communication between themselves. There is no central authority that can make decisions on behalf of other actors, all are equal, so-called "peers".

This means, for example, that there is no "cloud" or any other central server in the system.

Using the Blockchain, we can construct systems of information, processes and apps that are rooted in a digital ID owned and controlled by the individual. The applications in such a system are called Decentralised Apps and communicate with other dApps and other players in the system directly peer-to-peer, ie without going through any central server.

The information is stored encrypted in common by all actors on the network, such that only the information owner can compile and unlock the complete information.

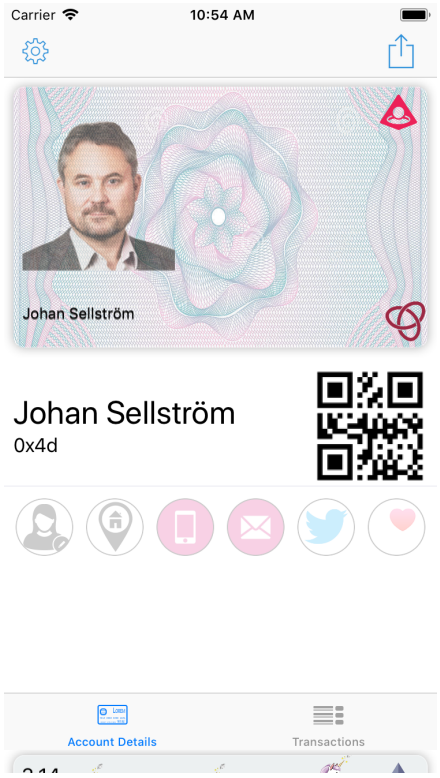
Information in existing systems can be cryptographically linked to the digital identity and thus signed into the blockchain and thereby, during a transition period, remain in the original system while retaining the same authenticity guarantees.

CareChain - A National Block Chain for Health

CareChain provides the necessary infrastructure to enable future decentralised health solutions where the individual owns and controls their own data. CareChain is a platform for innovation where both healthcare and the major ecosystem of independent app and system developers in health can begin experimenting with the new protocols the chain chain offers.

Individual Self-Owned Digital ID

A central part of CareChain is a built-in digital ID that is controlled by the individual. This ID is a set of standardised Smart Contracts on the Blockchain and can be used such as via a mobile app to authenticate against the services built on CareChain.



Guaranteed, Integrated Information Integrity

All information stored in CareChain is digitally signed on the Blockchain and cannot be manipulated. All CareChain actors can independently verify that the information is authentic.

Built-in policy guarantees with traceability

Information flows and other rules or agreements on how communication between parties on CareChain are described in the Smart Contracts that ensure compliance. All activity such as the creation of new information, sharing of information, etc. takes place in the form of transactions on the Blockchain, resulting in a cryptographically signed activity log over everything that has occurred

in the system.

The advantages of a consortium

A consortium can establish a blockchain to which everyone can connect, but where only members, independent organisations who enjoy public trust, are jointly responsible for the computers (nodes) that verify the transactions. In other words, the nodes managed by the consortium members guarantee network integrity. To falsify the information in a consortium chain such as CareChain would require an attacker to break in to a majority of consortium members, which in practice would be nearly impossible, or that more than half of the organisations would agree to rewrite history and thus individually risk their public trust.

In contrast, today's *public blockchains* use a model for verifying transactions based on the so-called mining nodes individually solving calculation-intensive problems, known as proof-of-work. This model limits the chain capacity and can introduce a latency which is inappropriate for the transaction volumes that CareChain will handle. Additionally, use of today's public blockchain offers no way to ensure that the information on the Blockchain stays in a particular geographical region.

The CareChain consortium requires no *mining*, as members trust each other and can be held legally responsible for deviations from this agreement. The capacity to handle large transaction volumes is thereby dramatically increased and the unfortunate ecological side effect in terms of significant energy usage, as required by *proof-of-work verifications is also avoided*.

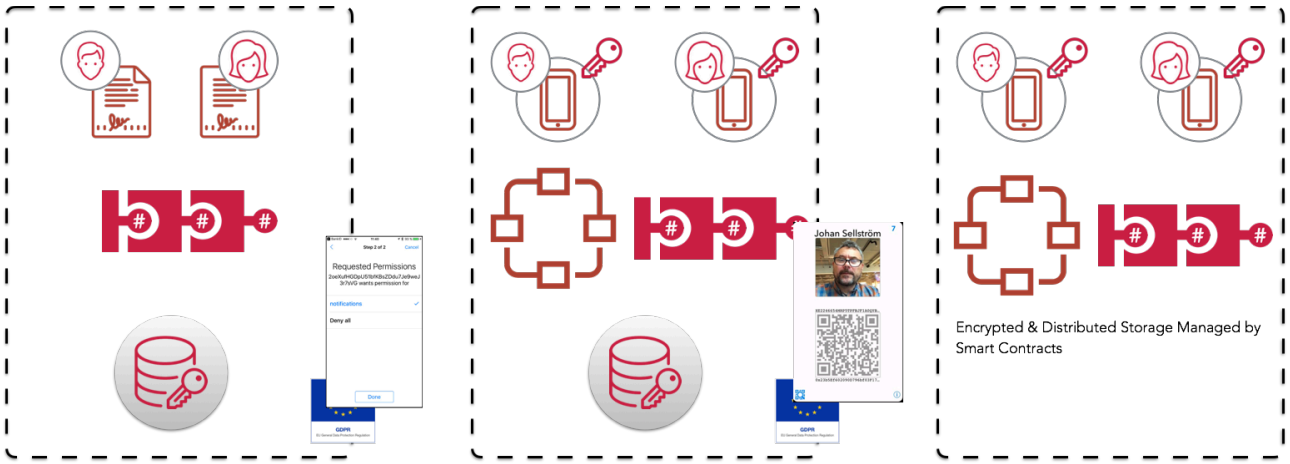
The Data Protection Regulation GDPR

The new EU Data Protection Ordinance (GDPR), which enters into force in May 2018, places higher demands on companies and organisations that handle personal data in general. This leaves very limited time to adapt to existing routines and systems, and to live up to this EU common law is expected to be a challenge not only for care but for society as a whole.

The Blockchain is expected to be a key component of the institutions, systems and mechanisms required to comply with data protection regulations and guidelines such as GDPR. Furthermore, it enables an effective framework for managing and securing personal data in general, where the information owner has actual control of how the information is used (owner). CareChain contributes by providing a powerful innovation platform for new health and healthcare solutions. We believe solutions built on CareChain will be well prepared for GDPR compliance because the infrastructure itself puts the patient, as the owner of the information, in the center. In order to confirm this hypothesis, a demonstrator that addresses the key challenges will be presented and subjected to the inspection by the Swedish Datainspektionen.

Enabling decentralisation

The new decentralised architectures necessary for the new data protection requirements will not be immediately adopted by all incumbents. However, CareChain is uniquely positioned to develop support for several of the GDPR directives such as Dynamic Consent Management and Right to Data Portability. This makes for a natural transition to go distributed.



Semantic and Dynamic Consent Mangement

Data Export

Distributed Master Data

Well ahead of the critical May 25th, 2018 date, Consent Management and Data Export/Import will be our first market offerings to bootstrap the CareCoin token.

Summary

CareChain is the only consortium of its kind in the Nordic region (and the world?). It represents a completely new decentralised data platform for health data that is not owned or controlled by any individual organisation but which puts the individual at the center and addressable by identity not location. By being completely open and politically neutral, both the major system suppliers to healthcare as well as app developers can experiment with the new protocols. CareChain consortium participation generates strong network effects in more rapidly developing a new architecture that integrates individual and health-generated data under the control of individuals and in harmony with GDPR . At the same time, the opportunity to create benefits for other actors is opened by sharing health data, in plain text or anonymised in social groups for analysis or investing data in clinical research pro-bono or for token profits.