A Decentralized Healthcare Insurance Protocol

Abraham Nash

1.1 Decentralized Insurance Solution

In return for access to learning on personal health information stored on a patient's PHR, a fungible store of value is deposited directly into patients' digital wallets (without a third-party mediator). AI developers use ERC-20 tokens to access on-chain smart contracts which coordinate the federated learning process with patients' personal data stores.

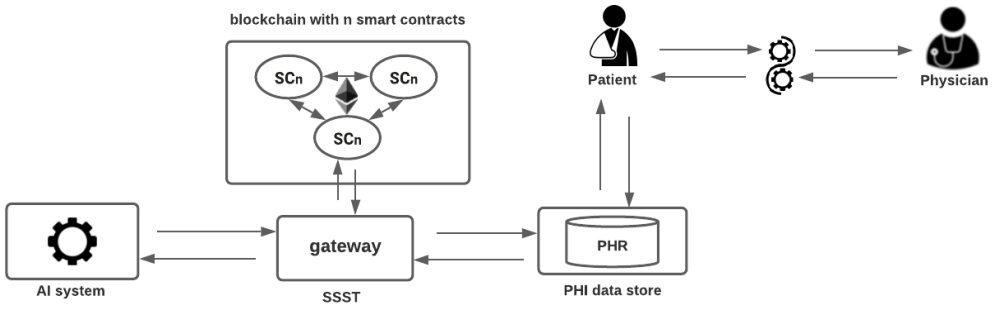

Figure 1. The rewards mechanism of cryptographic insurance in a learning health system.

A patient and physician establish the setup of healthcare as described in sections 1 & 2. A physician records personal health information into a patient-owned PHR as in HIE of One as described in section 2. An ERC-20 token accesses FL protocols on-chain to train a model on PHI to develop AI tools in healthcare. Tokens are deposited directly into patients' decentralized identity wallets (e.g., Tally Ho, etc.) upon successfully submitting a model update to a FL round. A patient uses these ERC-20 tokens to purchase decentralized insurance premiums, which fund and/or subsidize the provision of health care, and the cycle continues.

In FL, the literature shows that the amount of data is the most valuable in the training of machine learning algorithms [cite - fabio]. Patients with ongoing healthcare conditions will typically have more PHI in their health records. This is because they require more healthcare. This means, that they are more likely to receive greater rewards in the learning process. As they will require more expensive insurance premiums, this suits itself well to the mechanism outlined in Section 3.4 in a decentralized intelligence health network [decentralized insurance premiums].

1.2 Decentralized Insurance Premiums

1. Product Designers
2. Oracle: The physician in this sense?
3. License Provider. Healthcare Actuary?
4. Distributor Registry. Unsure yet.

1.3 Patients: Verification of insurance

The automated verification process of health care insurance claims can be handled better on the blockchain as it provides a reliable source of information with which to verify information and insurance credentials [1].

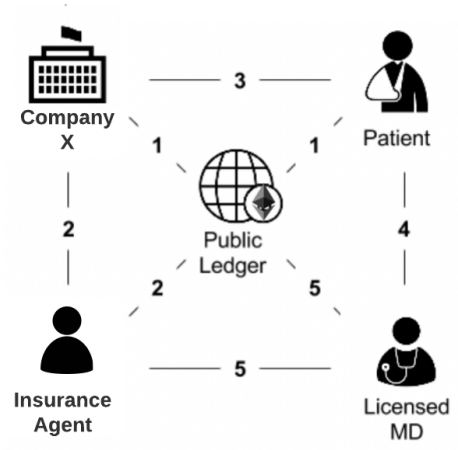

Figure 2 An example of patient use of a decentralized insurance service. Adapted from HIE of One. []

To preserve the privacy of personal information in the claims process, specific aspects of a DID can be encapsulated by the DecIdM service through a method known as zero-knowledge proof (ZKP) [2]. In short, ZKP would allow a patient to prove an aspect of their identity without requiring any specific information of that aspect to be disclosed to other parties. One way ZKP can be implemented in DID systems is to delegate the verification tasks to a number of trusted authorities (e.g., a government office or a notary service), who each holds a respective DID. Any authority selected by the DID holder can provide a certificate of their claim along with a signature generated from the authority's DID and an expiration date of the certificate. The certificate and its expiration date will be recorded in the blockchain (equivalent to a record of some cryptocurrency exchange) and attached to the DID of the owner making the claim. The signature from the authority can be verified using cryptography, just like the verifications of signatures in a cryptocurrency blockchain [3]. The DID owner can then share the certificate with any other user to prove the possession of a certain aspect of their identity. In doing so, both the claim initiator and the verifier of the claim are liable for the certification process in case of any dispute. Although ZKP might not be a required component, most DecIdM systems implement ZKP or other cryptographic techniques to protect user privacy.

Here is a simple example demonstrating how ZKP would work: suppose that DID holder Alice would like to establish an aspect of her identity as an insured patient by claiming that she currently receives healthcare insurance benefits from Company X in order to receive care. Alice can request Company X to serve as her certifying authority for the insurance claim. Alice may contact Company X offline to provide the required information (or other certificates already established as part of her DID). The insurance agent completes the verification of the documents offline, they can issue a formal verification of Alice's current insurance enrollment by signing the certificate with an expiration. This record is logged in the blockchain transaction list and linked to Alice's DID. Alice is now able to share her DID with a new certificate showing her proof of insurance coverage to any healthcare professional she chooses, without the need to disclose personally identifiable information such as her social security number and date of birth.

Although blockchain-based DID solutions remove much of the dependency from intermediaries in principle, some degree of centralization necessarily remains such as during the beginning phases of identity establishment. For instance, in order to prove an attribute of a patient's identity (e.g., insurance enrollment), the patient must create a claim upfront that is then verified by some trusted authority or notary service (e.g., the insurer). This formal verification is necessary to produce a credential ensuring non-repudiation of the patient's identity attribute. The credential will be reusable within the expiry, but its initial acquisition relies on trusted services being available. As a result, the availability of any DID system especially during its early adoption would inevitably be affected by the availability of those services.

3.6 Claims Process

The verification process to ensure a patient has insurance enables care to proceed. Upon receiving care, personal health information(PHI) is deposited into a patient-owned health record. This information serves as the basis for making a claims request to reimburse the physician and adjacent services for their services. Traditionally, the physicians/provider would handle this process - they only need to verify that the patient has healthcare insurance before they deliver their services. Although, this is not always straight forward and sometimes unexpected co/pays and deductibles incur unexpected fees and payments the patient needs to make. This is because the provider controls access to the patient's health information and is responsible for issuing the claims process. Instead of raw personal health information, the provider will use "codes" to represent the health conditions of insured patients. Taking the US as an example, these codes represent the health condition being treated with a variety of attributes and sub-categories. The physician/provider then reimburses their expenses and bills the patient for any co-pays and/or deductibles to make up the difference. The physician requests permission from the patient to issue a claims process using coded criteria.

Who are the claims assessors?
There are two main approaches to claims assessment using blockchain technology. Firstly, using an oracle which is either a trusted off-chain information provider (eg to trigger parametric insurance events) or secondly, crowd-sourcing information and assessing claims using voting mechanics (eg a prediction market).

There are two main approaches to claims assessment using blockchain technology. Firstly, using an oracle which is either a trusted off-chain information provider (eg to trigger parametric insurance events) or secondly, crowd-sourcing information and assessing claims using voting mechanics (eg a prediction market). Under a discretionary mutual model there is a legal requirement that a group or subgroup of members decide on how funds are distributed.

Slashing

Similar to Nexus mutual model? https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf
Returning to the crowd-sourced model, there needs to be an incentive for people to report and **a strong disincentive to prevent fraudulent reporting**. This is somewhat difficult to achieve in an insurance context because there is a clear incentive to defraud the pool by 1) purchasing cover for a low percentage of the cover amount, 2) using a substantial portion of the cover amount to pay-off claims assessors and then 3) pocketing the difference. A solution to this issue is to require claims assessors to have a significant stake in the success of the overall pool and a high disincentive to act dishonestly. This can be achieved by requiring a stake to be posted in the form of membership tokens. The stake is deposited for a specified period of time and provided claims are assessed honestly it is returned. If **the Advisory Board deems a claims assessor to be acting dishonestly it has the power to burn the staked member tokens**.

Doctors Collude
Slash doctors. Physicians ARE the oracles. They supply the data i.e. PHI. Patients can be provers of the information they hold? They are most likely to collude as they have the power to insert false information and submitifor a claims process.
Say I'm a physician and I set up 100 patient accounts. I can use those accounts to supply PHI, submit codes of health criteria, make a claim, and receive payment on insurance premiums.
Can doctors and patients collude?
I write into your record, I make a claim for you. I give you 'x' amount (based on trust). In this case, it is still the doctor who is the driver of fraudulent activity, and responsible for issuing the rewards process. In a real-world scenario, a physician is incentivized to not get slashed as they are seeking reimbursement from insurers for the services they will have already provided - it still remains that the physician gets slashed.

1.4 Verification in the Claims Process

Personal health information(PHI) is sensitive information and needs to be handled in a confidential manner. Equally, the code criteria for the health conditions issued by physicians need to be verified to meet the criteria of the premium that was purchased for a pay-out to occur.
Code criteria are useful as they are small units of data that can be used to represent health conditions and services being claimed for and using ZK-Proofs these can be put on-chain. However, there remains a problem of confidentiality. A Prover may wish to redact or modify sensitive data before presenting it to a Verifier. Digital signatures are designed specifically to invalidate modified data, however. They thus prevent a Prover from making confidentiality-preserving alterations to data. (See Section 7.1

for more discussion.). 6.2 DECO and Town Crier DECO [234] and Town Crier [233] are a pair of related technologies currently being developed in Chainlink networks [**DECO Chainlink**: https://chain.link/whitepaper].

Most web servers today allow users to connect over a secure channel using a protocol called Transport Layer Security (TLS) [94]. (HTTPS indicates a variant of HTTP that is enabled with TLS, i.e., URLs prefixed with "https" denote the use of TLS for security.) Most TLS-enabled servers have a notable limitation, though: They don't digitally sign data. Consequently, a user or Prover cannot present the data she receives from a server to a third party or Verifier, such as an oracle or smart contract, in a way that ensures the data's authenticity. Even if a server were to digitally sign data, there remains a problem of confidentiality. A Prover may wish to redact or modify sensitive data before presenting it to a Verifier. Digital signatures are designed specifically to invalidate modified data, however. They thus prevent a Prover from making confidentiality-preserving alterations to data. (See Section 7.1 for more discussion.)

DECO and Town Crier are designed to allow a Prover to obtain data from a web server and present it to a Verifier in a way that ensures integrity and confidentiality. The two systems preserve integrity in the sense that they ensure that data presented by the Prover to the Verifier originates authentically from the target server. They support confidentiality in the sense of allowing the Prover to redact or modify data (while still preserving integrity). A key feature of both systems is that they do not require any modifications to a target web server. They can operate with any existing TLS-enabled server. In fact, they are transparent to the server: From the viewpoint of the server, the Prover is establishing an ordinary connection. The two systems have similar goals, but differ in their trust models and implementations as we now briefly explain.

Conclusion

Decentralized insurance protocols are well suited to enhance the functions of more cost-effective and reliable coverage schemes. In addition to a value exchange for the use of a patient's computational resources and access to their personal health data, funding is required for health care services and treatment. A long-term roadmap scales a reduction in the costs of healthcare insurance, lowering the cost of entry to provision and increasing access to healthcare

[1] P. Zhang and T.-T. Kuo, "The Feasibility and Significance of Employing Blockchain-Based Identity Solutions in Health Care," in *Blockchain Technology and Innovations in Business Processes*, S. Patnaik, T.-S. Wang, T. Shen, and S. K. Panigrahi, Eds. Singapore: Springer, 2021, pp. 189–208. doi: 10.1007/978-981-33-6470-7_11.

[2] Rackoff, C., Simon, D.R.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Annual International Cryptology Conference, pp. 433–444. Springer, Berlin (1991).

[3] Narayanan,A.,Bonneau,J.,Felten,E.,Miller,A.,Goldfeder,S.:BitcoinandCryptocurrency. Technologies: A Comprehensive Introduction. Princeton University Press (2016)