A Decentralized Healthcare Insurance Protocol

Abraham Nash

abrahamnash@protonmail.com

This decentralized health insurance protocol expands on the idea of integrating healthcare insurance in a more community-driven way. Instead of individuals managing their own data, the protocol pools data within communities using the DHIN infrastructure [1]. This model aims to more effectively fund decentralized health insurance pools, creating a system that benefits the collective well-being of the community.

1.1 Decentralized Insurance Solution

In exchange for access to health data stored on a patient's Personal Health Record (PHR), a fungible store of value (e.g., RAI, DAI, USDT) is deposited directly into the patient's digital wallet, without any third-party mediator. AI developers use ERC-20 stablecoin tokens (e.g., RAI, USDT) to compensate patients for granting access to their data, which is facilitated through on-chain smart contracts. These smart contracts coordinate a decentralized federated learning process, allowing AI models to be trained without centralized access to sensitive personal health data, ensuring privacy while enabling data-driven innovation.

AI system DID and utilisation of such gateways to interact with patient data stores as led by clinicians is elaborated on in Decentralized Healthcare Intelligence Network (DHIN).

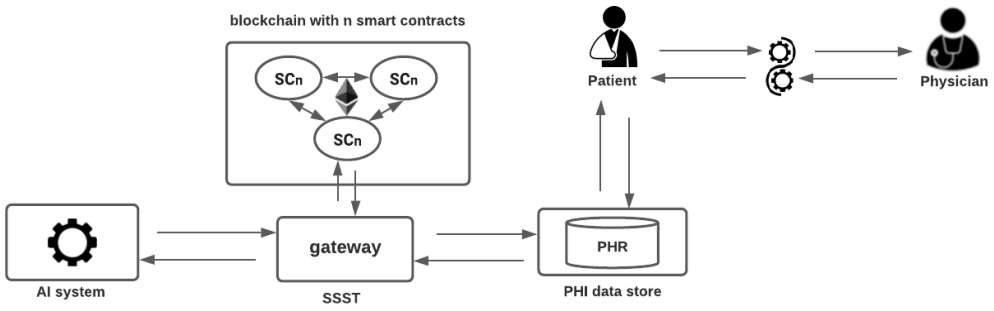

Figure 1. The rewards mechanism of cryptographic insurance in a learning health system.

A patient and doctor collaboratively establish the healthcare setup, where the doctor records health data in a patient-owned Personal Health Record (PHR). In return for allowing an AI system to access federated learning (FL) protocols on-chain and train a model using the patient's health data, ERC-20 tokens (e.g., RAI, USDT) are rewarded to the patient. These tokens are directly deposited into the patient's decentralized identity wallet (e.g., MetaMask, TaHo) after the successful submission of a model update to an FL round. Patients can then use these rewards to purchase decentralized insurance premiums, which either fund or subsidize their healthcare provision. This creates a continuous cycle of incentivized data-sharing and healthcare funding.

In the context of Federated Learning (FL), the volume of data plays a critical role in training machine learning models [1] (Fabio et al.). Patients with ongoing healthcare conditions tend to accumulate more health data due to their frequent medical visits, making them more likely to receive higher rewards in the learning process. This dynamic aligns well with their situation, as these patients often face higher insurance premiums. In essence, patients with greater healthcare needs are not only more likely to be reimbursed more frequently but are also expected to receive rewards that reflect their higher healthcare utilization.

1.2 Decentralized Insurance Premiums

1. Insurance Premium: Product Designers
2. Oracle: Medical Professional

3. License Provider: Healthcare Actuary
4. Distributor Registry: On-Chain Smart Contract.

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].

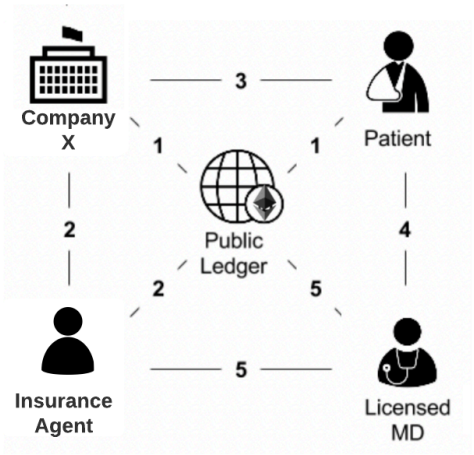

Figure 2 An example of patient use of a decentralized insurance service. Adapted from HIE of One. []

To preserve the privacy of personal information in the claims process, specific aspects of a decentralized identity (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 hold 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 date. 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.

1.4 Claims Process

The verification process to ensure a patient has insurance is critical for allowing care to proceed. Upon receiving care, health data is recorded into a patient-owned health record, which serves as the basis for making a claims request to reimburse the doctor and adjacent services for their provided services. Traditionally, the doctor/provider handles this process, as they only need to verify that the patient has healthcare insurance before delivering their services. However, this process is not always straightforward, as unexpected co-pays and deductibles may result in fees and payments that the patient must cover. This is due to the fact that the provider controls access to the patient's health information and is responsible for initiating the claims process.

Instead of using raw personal health data, the provider employs "codes" to represent the patient's health conditions. For instance, in the US, these codes specify the health condition being treated and include various attributes and sub-categories. The provider then reimburses their expenses and bills the patient for any co-pays or deductibles that help make up the difference. Before proceeding, the doctor requests permission from the patient to initiate the claims process, typically using these coded criteria.

1.4.1 Who Are the Claims Assessors

There are two primary approaches to claims assessment using blockchain technology. The first approach involves using an *oracle*, which is a trusted off-chain information provider that can trigger parametric insurance events. The second approach is crowd-sourcing information and assessing claims using voting mechanisms (e.g., prediction markets).

Under a discretionary mutual model, a legal requirement mandates that a group or subgroup of members decide how funds are distributed.

1.4.2 Slashing and Nexus Mutual Model

Returning to the crowd-sourced model, an incentive structure is needed to encourage people to report honestly and create strong disincentives against fraudulent reporting. This is especially challenging in an insurance context, as there are clear incentives for fraud. For example, a fraudulent participant might purchase coverage for a small portion of the total coverage amount, then use a significant portion of that cover to pay off claims assessors, and pocket the remaining difference.

A solution to this problem is to require claims assessors to have a substantial stake in the overall success of the pool. By doing so, the disincentive for dishonesty is strengthened. This can be achieved by requiring assessors to post a stake in the form of membership tokens, which are deposited for a specified period. Provided claims are assessed honestly, the stake is returned. If the "Advisory Board" deems a claims assessor to be dishonest, they have the power to burn the staked tokens, essentially slashing the assessor.

1.4.3 Slash Doctors

In this framework, doctors act as oracles, verifying or affirming the health data provided when they deliver care. This can include generating the need for tests and prescriptions or assigning diagnostic codes to represent the health data of patients. Patients, in turn, can serve as "provers" of the information they hold, though there is a risk of collusion, especially since patients have the ability to submit false information as part of the claims process.

For example, consider a scenario where a doctor sets up 100 patient accounts and uses those accounts to provide health data, submit health condition codes, file a claim, and receive payment from insurance premiums. In such cases, proof of "patienthood" becomes essential — a method of decentralized verification is necessary to ensure the patient's identity and legitimacy of their health data. Proof of "doctorhood" can be established by associating a decentralized identifier (public/private key pair) to a doctor's credentials, a method that has already been demonstrated.

1.4.4 Doctors and Patients Collusion

In a scenario where a doctor writes into a patient's record and files a claim on their behalf, they could offer the patient a share of the fraudulent claim (based on mutual trust). However, in this case, it is still the doctor who drives the fraudulent activity and is responsible for issuing the reward process. Such practices can already occur in traditional insurance models.

In a real-world scenario, doctors are incentivized not to engage in fraudulent activities, as doing so would jeopardize their ability to secure reimbursement from insurers for the services they provide. This creates a system where doctors are motivated to act ethically to avoid being slashed and to maintain their relationship with the insurance providers.

1.5 Verification in the Claims Process

Health data is inherently sensitive, and it must be handled with strict confidentiality. Likewise, the code criteria for health conditions, issued by doctors, must be verified to ensure they meet the requirements of the premium purchased in order for a payout to occur.

Code criteria, which include ordered investigations, treatments, and non-diagnostic information, are valuable because they represent small units of data that can be used to reflect health conditions and services being claimed. Using Zero-Knowledge Proofs (ZK-Proofs), these data can be placed on-chain. However, a challenge remains around maintaining confidentiality. A Prover may want to redact or modify sensitive data before presenting it to a Verifier. While digital signatures are specifically designed to invalidate modified data, they prevent the Prover from making alterations to the data that would preserve confidentiality.

1.5.1 DECO and Town Crier

DECO and Town Crier are related technologies currently under development within the Chainlink network [5]. They address the challenge of ensuring both data integrity and confidentiality.

Most modern web servers allow users to connect via a secure channel using a protocol called *Transport Layer Security*(TLS). URLs prefixed with "https" indicate that TLS is in use, ensuring data security during transmission. However, most TLS-enabled servers have a significant limitation: they do not digitally sign the data. As a result, a Prover cannot present the data they receive from a server to a third-party Verifier, such as an oracle or a smart contract, in a way that guarantees the authenticity of the data.

Even if a server did digitally sign its data, confidentiality issues would still arise. A Prover may wish to redact or modify sensitive data before sharing it with a Verifier. While digital signatures are designed to detect and invalidate altered data, they make it impossible for a Prover to make confidentiality-preserving changes.

1.5.2 How DECO and Town Crier Work

DECO and Town Crier were specifically designed to allow a Prover to obtain data from a web server and present it to a Verifier in a manner that guarantees both integrity and confidentiality. These systems ensure data integrity by confirming that the data the Prover presents to the Verifier originated authentically from the target server. They support confidentiality by allowing the Prover to redact or modify the data, while still preserving its integrity.

A key advantage of both DECO and Town Crier is that they do not require any modifications to the target web server. These systems operate transparently, meaning that from the server's perspective, the Prover is simply establishing an ordinary TLS connection. This enables seamless integration with existing TLS-enabled servers, without any need for changes to the server itself.

2. 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

References

[1] Nash, A. (2023). **Decentralized Health Intelligence Network**. *arXiv*. Available at: https://arxiv.org/abs/2408.06240.

[2] Amato, F., Qi, L., Tanveer, M., Cuomo, S., Giampaolo, F., & Piccialli, F. (2023). *Towards One-shot Federated Learning: Advances, Challenges, and Future Directions*. Available at: https://arxiv.org/pdf/2505.02426.

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

[4] Rackoff, C., & Simon, D. R. (1991). *Non-interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack*. In *Annual International Cryptology Conference* (pp. 433–444). Springer, Berlin.

[5] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

[6] DECO Chainlink Whitepaper. Available at: https://chain.link/whitepaper.