A Decentralized Healthcare Insurance Protocol

By Abraham Nash
abrahamnash@protonmail.com

Abstract

This paper examines decentralized insurance protocols in healthcare, focusing on their capacity to deliver cost-effective coverage and patient compensation for data use. Utilizing blockchain, these protocols aim to lower healthcare costs and administrative burdens while safeguarding patient data privacy through advanced technologies like Zero-Knowledge Proofs. Central to this approach is the empowerment of patients, granting them greater autonomy over their health records and financial interactions. The anticipated outcome is a more accessible and equitable healthcare system, primed for future advancements and broader patient inclusion.

1.1 Decentralized Insurance Solution

The healthcare industry stands on the cusp of transformation with the integration of decentralized insurance solutions. In this emerging model, patients receive a tangible incentive, such as a fungible store of value like DAI, in exchange for contributing to the collective intelligence of healthcare data. This value is transferred directly to patients' digital wallets, bypassing the need for intermediary financial institutions.

AI developers and healthcare researchers tap into this wealth of anonymized patient data by utilizing ERC-20 tokens. These tokens grant them access to on-chain smart contracts, which in turn orchestrate a decentralized federated learning ecosystem. By engaging with patients' personal data stores in this manner, the learning process respects patient autonomy and privacy while still benefiting from the aggregate data insights.

This novel approach paves the way for a reciprocal relationship between data contribution and compensation, fostering a learning health system that rewards patient participation. Moreover, it underscores the transition from traditional, centralized health data management to a patient-empowered model that aligns with the ethos of blockchain technology – transparency, security, and equity.

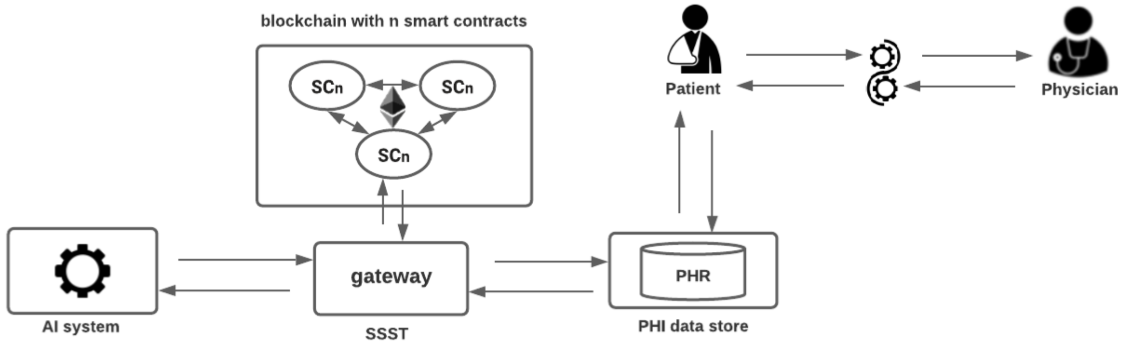

Figure 1: The Rewards Mechanism of Cryptographic Insurance in a Learning Health System

Figure 1 depicts a sophisticated blockchain-enabled ecosystem designed to facilitate interactions between patients and physicians within a learning health system. At the heart of this system lies a secure gateway, likely a component of the Server-Side Security Token (SSST), which manages access to Personal Health Records (PHRs). These records are stored in a way that ensures patient confidentiality while still allowing for valuable health data to be utilized for learning purposes.

The system integrates an Artificial Intelligence (AI) module, suggesting its role in analyzing health data to derive actionable insights. This AI component is connected through the secure gateway, indicating a safeguarded passage for data flow. The blockchain framework, illustrated with multiple smart contracts (SCn), is central to this model, indicating a structure where transactions and interactions are not only automated but also reinforced with the inherent security protocols of blockchain technology.

Smart contracts within this environment represent the automated agreements that enable the rewards mechanism, which likely involves the exchange of value for access to anonymized health data. The implication is a self-executing, cryptographic insurance model where contributions to the health data pool are directly incentivized, promoting a participatory approach to health data sharing and learning.

1.2 Participatory Health Data Economy and Federated Learning

In the proposed decentralized healthcare system, the relationship between a patient and a doctor is fundamental to the setup of healthcare provision. Upon each interaction, doctors input health data into a patient-owned Personal Health Record (PHR). This action triggers a sequence within the blockchain framework where patients are compensated with ERC-20 tokens like DAI for granting an AI system the right to engage with Federated Learning (FL) protocols on-chain. This permission allows for the patient's health data to contribute to the training of machine learning models, which are then used to further develop AI tools in healthcare.

The compensation mechanism is direct and secure, with tokens being deposited into the patient's decentralized identity wallet—such as Tally Ho—following their contribution to a model update in an FL round. These tokens serve a dual purpose: they can be utilized by patients to purchase decentralized insurance premiums, thus facilitating the funding and subsidization of their healthcare needs. This establishes a sustainable cycle of data sharing, compensation, and healthcare provisioning.

Federated Learning literature highlights the value of data quantity in enhancing machine learning algorithms [citation needed]. Patients with chronic health conditions, who naturally accumulate more health data due to frequent healthcare interactions, stand to gain more from this system. Their substantial health records position them to earn greater rewards in the learning process, which is particularly advantageous given their likely need for higher insurance premiums. This correlation creates a virtuous cycle, aligning the economic incentives of the health data economy with the healthcare needs of patients.

1.3 Decentralized Insurance Premiums

Within the framework of a decentralized healthcare system, insurance premiums are reimagined to align with the principles of blockchain technology, offering a more equitable and transparent mechanism for managing healthcare costs.

1.3.1 Product Designers

Product designers in a decentralized insurance protocol are responsible for creating insurance products that are not only financially viable but also meet the specific needs of the patient population. They craft the terms and benefits of insurance coverage, utilizing smart contracts to encode these details into the blockchain. This ensures that the insurance products are consistent, transparent, and tamper-proof. In this ecosystem, product designers must consider the dynamic nature of health data and the direct relationship between patient data contribution and insurance benefits.

1.3.2 Oracle: The Doctor's New Role

In decentralized systems, oracles serve as bridges between blockchain and real-world data. Doctors could assume the role of oracles, verifying healthcare events and outcomes that trigger insurance claims or premium adjustments. As trusted healthcare providers, their attestations would carry significant weight, ensuring that the insurance protocol operates on accurate and timely information. This setup also has the potential to streamline claim processes, reduce fraud, and increase efficiency.

1.3.3 License Provider: The Healthcare Actuary

Actuaries in traditional insurance use historical data to predict risk and set premiums. In a decentralized healthcare system, the healthcare actuary's role expands to include the licensing of insurance products on the blockchain. They would analyze health data and FL model outputs to assess risk profiles more accurately, potentially in real-time. This would allow for more personalized, fair, and responsive insurance premiums, shifting the actuarial process from a predictive model to an adaptive, learning model.

1.3.4 Distributor Registry: A New Paradigm

The Distributor Registry would act as a decentralized marketplace for insurance products, where patients can browse and select the insurance plans that best fit their needs and rewards status. It's a platform that would require careful consideration and design, as it needs to uphold the highest standards of security and privacy while offering a user-friendly interface for patients and providers alike. This registry could be curated by patient feedback, AI recommendations, and actuarial inputs, ensuring that it remains up-to-date with the best available insurance options.

1.4 Patients: Verification of Insurance

The blockchain offers an innovative solution for the automated verification of healthcare insurance claims, serving as a reliable and immutable ledger for validation purposes. To maintain the confidentiality of personal information during the claims process, Decentralized Identity Management (DecIdM) services can implement a method known as Zero-Knowledge Proof (ZKP).

ZKP allows patients to confirm aspects of their identity or claim without disclosing the actual data associated with it. Within decentralized identity (DID) systems, ZKP can be operationalized by assigning verification responsibilities to a consortium of trusted authorities, each possessing a unique DID. These entities, which could range from government offices to notary services, provide a verifiable certificate with an accompanying signature and expiry date, anchored to the patient's DID on the blockchain.

This certificate functions as a testament to a particular aspect of the patient's identity, much like a record in a cryptocurrency ledger. The cryptographic signature from the authority is verifiable using the same principles that secure transactions on a cryptocurrency blockchain. Patients can then present this certificate to any other party to substantiate a claim of identity or insurance coverage.

In this system, the burden of liability in the certification process is shared between the claimant and the verifier, ensuring accountability in the event of disputes. While ZKP may not be necessary for all DecIdM systems, its implementation, along with other cryptographic techniques, is crucial for safeguarding user privacy in the evolving landscape of decentralized healthcare.

In the realm of decentralized identity (DID) verification, Zero-Knowledge Proof (ZKP) offers a compelling solution for asserting insurance coverage while preserving the anonymity of the insured. Here is a practical illustration of how ZKP facilitates this process:

Consider Alice, a DID holder, who needs to confirm her status as an insured patient with healthcare benefits from Company X. Alice opts for Company X to act as her certifying authority. To initiate this process, Alice may provide necessary evidence or pre-existing certificates associated with her DID to Company X through secure, offline channels. Once the insurance agent at Company X authenticates Alice's documentation, they can issue a formal certificate verifying Alice’s insurance status. This certificate is digitally signed and given an expiration date, becoming part of the blockchain transaction ledger and linked to Alice's DID.

Now, Alice possesses a verifiable certificate within her DID that attests to her insurance coverage. She can present this certificate to any healthcare provider, proving her insured status without revealing sensitive personal information such as her social security number or date of birth. This mechanism exemplifies the power of ZKP in action—allowing for verification without compromising privacy.

However, while blockchain-based DID systems significantly reduce reliance on intermediaries, a certain degree of centralization persists, particularly during the initial stages of identity verification. For a patient to authenticate an attribute like insurance enrollment, they must first create a verifiable claim, typically certified by a recognized authority or notary service, such as the insurance company itself. This initial validation step is essential to generate a non-repudiable credential that confirms the patient's identity attribute. While the credential is reusable until its expiration, obtaining it initially depends on the presence and accessibility of these authoritative services. Therefore, the early adoption and overall availability of a DID system are inherently linked to these central verification entities' capacity to provide such services.

2.1 Claims Process

The claims process in a decentralized healthcare system is designed to streamline the verification of insurance coverage and facilitate the reimbursement for services rendered. When a patient receives care, the pertinent health data is securely logged into their personal health record (PHR). This data forms the foundation for initiating a claims request.

Traditional Claims Handling

Conventionally, healthcare providers are responsible for initiating the claims process. Their primary task is to ensure that the patient holds valid insurance coverage before services are delivered. However, this process can become complex, often leading to unanticipated out-of-pocket expenses such as co-pays and deductibles for the patient. This complexity arises partly because providers, who control access to the patient's health information, must translate medical conditions and treatments into standardized codes for billing purposes. In the United States, for instance, these coding systems are extensive and include a myriad of attributes and sub-categories. After providing care, the healthcare provider submits these codes to claim their fees and bills the patient for any remaining balances.

Decentralizing the Claims Process

In a decentralized system, the role of the healthcare provider shifts from being the sole custodian and initiator of the claims process to one of several participants in a more transparent and patient-centered model. The provider still requires permission from the patient to initiate a claim but does so using coded criteria that respect patient privacy and ensure accuracy in billing.
Claims Assessors in Blockchain

Blockchain technology introduces new methodologies for claims assessment:

- **Oracles as Assessors**: An oracle in blockchain parlance is a trusted entity that provides off-chain information. In the context of insurance, an oracle could be used to trigger parametric insurance events based on verified data inputs.
- **Crowdsourced Claims Assessment**: Another approach is to leverage the collective wisdom of a crowd through voting mechanisms, akin to a prediction market. Here, the assessment of claims is decentralized, and consensus-driven, allowing for more democratic and potentially unbiased adjudication.
- **Discretionary Mutual Model**: This model mandates that a group or subgroup of members within the network decide on the distribution of funds. Such a legal requirement ensures that the allocation of insurance payouts is governed by the collective agreement of the members, which can be facilitated by smart contracts on the blockchain.

The integration of these blockchain-based approaches offers a path toward more equitable, efficient, and transparent claims processes, shifting the power dynamics from traditional centralized entities to a more distributed and patient-empowering model.

2.2 Slashing Mechanisms in Decentralized Insurance

The concept of 'slashing' refers to the punitive measures taken against participants in a decentralized system who act dishonestly or maliciously. In the context of decentralized insurance, as outlined by the Nexus Mutual model, slashing serves as a crucial component to maintain the integrity of the system.

Incentivizing Honest Reporting

To encourage accurate claims reporting and deter fraud, there must be a system of incentives and disincentives. In an insurance pool, the potential for fraud exists when individuals purchase cover at a low percentage of the total value and then conspire with claims assessors to receive a disproportionate payout. To counteract this, claims assessors are incentivized to protect the overall pool's integrity by staking membership tokens as a guarantee of their honest participation.

Stakes and Penalties for Assessors

Claims assessors are required to deposit a stake in the form of membership tokens, which is locked for a predetermined period. This stake acts as collateral, ensuring that assessors act in the best interest of the mutual. Should assessors perform their duties honestly and in accordance with the established protocols, their stake is returned after the period ends. However, if the Advisory Board—which oversees the process—determines that an assessor has acted fraudulently, the assessor's staked tokens can be 'burned', meaning they are permanently removed or destroyed as a form of penalty.

The Role of Doctors as Oracles

In the proposed model, doctors act as oracles, affirming the validity of health data through their professional services—such as diagnostics and treatment codes. However, this system also presents a risk of collusion, particularly between patients and doctors, to submit false information for financial gain. To illustrate, a doctor could theoretically create multiple patient accounts to fabricate health data and file claims, exploiting the system for a payout.

Ensuring Proof of 'Patienthood' and 'Doctorhood'

To mitigate the risk of such collusion, robust verification mechanisms are required. 'Patienthood' must be proven, potentially through a decentralized verification method that ensures the authenticity of the patient's identity and their medical history. Similarly, 'Doctorhood' can be established by assigning a decentralized identifier—a public/private key pair—to a doctor's credentials, a method that has already been demonstrated in practice. This system would ensure that only verified healthcare professionals can act as oracles and that patients' claims are genuine.

2.2 Assessing the Risk of Collusion between Doctors and Patients

The potential for collusion between doctors and patients in fraudulent claims is a concern that any insurance system, decentralized or traditional, must address. The decentralized model, while innovative, is not immune to such risks and must consider the human elements of trust and dishonesty.

Dynamics of Fraudulent Claims

In the scenario where a doctor could write false information into a patient's health record and then initiate a fraudulent claim, the rewards from the claim could be shared between the doctor and the patient based on mutual trust. The doctor, as the initiator of this process, would be the primary driver of the fraudulent activity. While such collusion can occur in any insurance system, the decentralized nature of blockchain-based models raises specific challenges and opportunities for mitigating these risks.

Deterrents to Fraudulent Behavior

In a decentralized system, the concept of slashing, where an individual's stake or collateral can be forfeited as a penalty for dishonest actions, serves as a deterrent. For doctors, the risk of being slashed—losing their staked tokens or reputation within the system—provides a significant incentive to maintain honest practices. Additionally, doctors inherently seek reimbursement from insurers for the legitimate services they provide, which naturally aligns with the incentive to avoid fraudulent behavior.

Real-World Implications and Safeguards
In real-world applications, the risk of collusion is countered by a combination of ethical standards, legal repercussions, and the threat of losing one's professional license. In the decentralized context, these real-world deterrents are complemented by the technological safeguards of the blockchain, such as transparency, traceability, and the immutable recording of transactions. Moreover, smart contracts can be designed to require multiple independent verifications before releasing funds, thereby reducing the likelihood of successful fraud.

Ensuring Accountability
To further ensure accountability in the decentralized insurance model, a robust system of checks and balances can be implemented, including:

- **Auditing Mechanisms**: Regular audits by independent parties can detect anomalies in claims and trigger investigations.
- **Whistleblower Incentives**: Rewards for reporting suspected fraud can encourage community vigilance.
- **Reputation Systems**: A reputation system for both doctors and patients can track their history within the network, with consequences for those who attempt to defraud the system.

2.3 Verification in the Claims Process
The integrity and confidentiality of health data during the claims process are of paramount importance in a decentralized healthcare system. Verification of code criteria issued by doctors must align with the purchased insurance premium's terms to justify a payout.

Confidentiality and Verification Challenges
Code criteria, which encapsulate investigations, treatments, and other health-related services, can be efficiently represented by small data units. Implementing Zero-Knowledge Proofs (ZK-Proofs) allows these units to be verified on the blockchain without disclosing the underlying sensitive information. However, maintaining the confidentiality of this data poses a significant challenge. A Prover, such as a patient, may need to redact sensitive information before it is verified by a third-party or Verifier. The nature of digital signatures, which are designed to detect any modification to the data they secure, complicates this requirement for confidentiality.

DECO and Town Crier Solutions
To address these challenges, technologies like DECO and Town Crier, which are under development in the Chainlink network, are proposed as solutions. These systems are designed to fetch data from web servers securely and present it to a Verifier with both integrity and confidentiality intact.
Ensuring Data Integrity and Confidentiality

DECO and Town Crier enable a Prover to interact with any TLS-enabled web server, obtain data, and then present it to a Verifier while ensuring the data's origin is authentic and any redactions preserve the data's integrity. These technologies allow for confidentiality-preserving modifications—meaning a Prover can redact parts of the data without invalidating its authenticity.

Trust Models and Server Transparency
A notable feature of DECO and Town Crier is their compatibility with existing web infrastructure. They do not require any modifications to target servers and can operate with any TLS-enabled server. The systems are also server-transparent—meaning the server perceives the interaction as a standard connection. While DECO and Town Crier share similar objectives, they differ in their trust models and technical implementations,

Conclusion

Decentralized insurance protocols represent a transformative shift in the healthcare insurance landscape, offering a framework for more cost-effective and reliable coverage options. These protocols not only facilitate a value exchange for the utilization of patients' computational resources and access to their health data but also ensure that adequate funding is available for essential healthcare services and treatments.

The incorporation of blockchain technology and decentralized systems into the insurance sector promises to reduce administrative overhead, enhance data security, and streamline the claims process. This can lead to a significant decrease in the costs associated with healthcare insurance, thereby lowering the barriers to accessing healthcare services.

Moreover, as these decentralized protocols mature, we anticipate a broader impact on the healthcare system at large. The roadmap ahead envisions a scalable model where the efficiencies gained through decentralization lead to a tangible reduction in healthcare costs. This, in turn, expands access to quality healthcare, making it more inclusive and available to a wider population. The ultimate goal is a healthcare ecosystem that is not only more equitable but also sustains its improvements through continuous innovation and patient empowerment.

In this evolving paradigm, the patient is placed at the center of the healthcare equation, with an emphasis on privacy, autonomy, and participation in their healthcare decisions. The successful implementation of decentralized insurance protocols could herald a new era of healthcare provision, characterized by enhanced coverage schemes that are aligned with the needs and preferences of the patient community.

References

[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)