PDPM: A PATIENT-DEFINED DATA PRIVACY MANAGEMENT SYSTEM FOR DECENTRALIZED E-HEALTH ENVIRONMENTS UTILIZING NUDGES

[#1]**Mr.BOLLI RAMESH,** *Assistant Professor*

[#2]**Mr.DASARI SHANTHI KUMAR,** *Assistant Professor*

Department of Computer Science and Engineering,

SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Qualified healthcare organizations can access patient medical data via a blockchain-powered private decentralized ehealth ecosystem. The ledger permanently records all blockchain transactions. Each patient's privacy preferences are automatically saved by the eHealth system because they change regularly. Patients often change their privacy settings without consulting a doctor or other key person. We created, tested, and assessed PDPM, a user-defined nudging-based data protection mechanism for decentralized e-health systems, to solve these challenges. Patients can restrict medical record access. Smart contracts on the blockchain allow real-time data protection changes. User-defined, immutable data privacy helps ehealth organizations manage and adapt privacy. Authorized entities cannot dispute modifications because ledgers record all information. According to nudge theory, patients should receive the best privacy advice based on their behaviors, but they decide. Finally, we demonstrate how PDPM can enable user-defined data privacy control in decentralized eHealth systems.

***Keywords*:** blockchain, decentralized ehealth, data privacy management, nudge theory, smart contract, tamperproof data

1.INTRODUCTION

AI, IoT, blockchain, and robot technology can improve medical services and enable location- and time-independent, precise, and accurate medical planning. Commercial, academic, and healthcare groups have promoted multiple ways.Patient medical histories are essential to modern treatment. Electronic medical records (EMR), personal health records (PHR), continuity of care records (CCR), open electronic health records (open EHR), and others represent patient medical data that can be accessed online or offline (see Table 1). Security procedures for medical patient data access enable the ongoing growth of data from multiple sources. Patient data may be spread across multiple storage systems and services, making access challenging. Thus, the blockchain-based solution allows authorized parties to access data from numerous sources in one system. Thus, security, communication, and system efficacy are being evaluated more closely.

Hospital policies or healthcare stakeholders determine the default data privacy policy for each patient in e-health systems. Many default privacy standards exist in e-health environments, including and. The memo detailed a plan to safeguard the personal data and privacy of major eHealth and online booking platform users. Some e-health systems don't allow patients to change their privacy settings or provide fresh privacy updates for registered users. Traditional eHealth systems provide privacy updates. It is still done manually, and data is kept in an online and offline logbook that careless parties could change, causing future conflicts. Thus, eHealth requires an innovative approach that lets patients recommend routine privacy enhancements without third-party help. The latest privacy information is stored on

the blockchain.

To solve these difficulties, we offer PDPM, a collaborative system that uses nudge theory in decentralized e-health. PDPM gives patients the finest data privacy recommendations based on nudge theory data. The technology gives the patient full privacy control based on its recommendations. Additionally, the chosen data privacy management is onchain. Every modification is visible to confidential manager allowed organizations. Our open-source, decentralized Ethereum platform enables smart contracts.

Table 1 electronic health record data, storage, and transmission requirements.

Acronym	Description
CCR	Continuity of Care Record (Standard Specification)
CEN/TC 251	European Committee for Standardization
DICOM	Digital Imaging and Communications in Medicine
HL7/CDA/FHIR	Health Level-7. Fast Health Interoperability Resources.
HIPAA	Health Insurance Portability and Account- ability Act
ICD/ICF/ICHI	Family of International Classification
ICPC	International Classification of Primary Care
IHE [13]	Privacy Policies
ISO/TC 215 [14]	International Organization for Standard
LOINC [15]	Logical Observation Identifiers Names and Code
Open EHR [16]	Open Electronic Health Records
SNOMED-CT [17]	Systematized Nomenclature of Medicine

In conclusion, this research contributes:

Nudge the ory is used to build a secure architecture with patient-defined data privacy control indecentralized e-health environments.

Our decentralized e-health system offers the latest patient-defined data privacy protections.

The PDPM model is developed and tested using simulations.We have several observations and concerns based on our PDPM system modeling.

Organizational structure of the paper follows.

2.RELATED WORK

Industries, healthcare providers, and academic organizations have extensively researched decentralized centralized healthcare. Building a blockchain-based decentralized healthcare system has several techniques, concepts, and ambitions.

The nudge theory has also been applied to decision-making in FinTech, internet advertising, insurance, and open banking. In this chapter, we review previous research on decentralized e-health combining blockchain technology and nudge theory.We researched and proposed blockchain technology for PHI in 2018. Creating a reliable means for authorized organizations to access patient data is the main goal. Conventional PHI distributes and maintains patient data locally at internet-connected providers. In addition, patients lack complete information. The recommended plan can fix the concerns. Additionally, research in and has recommended comparative techniques and goals. Recent research suggests ssHealth, a blockchain-based, secure healthcare system. Edge computing and blockchain technologies were used to create an intelligent, secure healthcare system. Medical data can be safely exchanged between healthcare entities using the proposed method. A blockchain can record a person's lifetime health care journey and be shared with appropriate parties and authorized authorities, according to a patent. The systematic review is extensively covered in, and. Traditional cryptographic primitives and access control model design are used in many decentralized e-health research to manage data privacy. The authors proposed a revocable attribute-based signature for blockchain-based healthcare. The system needs coupling methods to protect user identification without a central authority. A second study proposed MediBchain, a blockchain platform with cryptographic protocols, to handle patients' confidential health information and ensure accountability, integrity, and security. In the interim, writers provided a cloud-based solution. Cloud-based encryption and pseudonymity encrypt patient data.

Nudge theory is mostly used in e-health to change patient behavior to treat them. A study using loss-framing to improve medical decision-making and patient exercise. To be healthy, cancer patients must follow their food and exercise routines. An incentive, a nudge method deployment, encouraged persistent physical activity. The author motivates patients to exercise by giving

them virtual rewards before the goal is reached, based on the notion that humans prefer to avoid losses to acquire benefits.

Through these methods, cardiovascular disease has improved.

3.TECHNICAL CHALLENGES

This section discusses the main technological issues that arise when adopting blockchain technology in e-health to ensure privacy and brevity. Nudging supports these obstacles.

Achieving Secure PatientDefined Data Privacy

The goal of this study is to create dynamic patient-defined data privacy management. Our approach uses nudge theory and blockchain technology to achieve the desired results. Managing patient data privacy throughout eHealth adoption may change. Data privacy control is critical in e-health contexts where only doctors, nurses, and others can read data. The information must be kept private. All users of the same private ehealth system can access insensitive data.

To achieve the patient's desired privacy management, data classification must precede nudge theory approaches. Medical care, clinical research, public institution, lifelog, and other data must be reviewed beforehand. Obtaining patient-defined cure data privacy is technical.

Nudge Theory in EHealth

Nudge theory, which improves ehealth patient care, is gaining popularity. Nudge theory is used to improve patient privacy management in our research. The vast amount of data and medical terminology that must be screened using an algorithm makes creating the nudge theory in decentralized ehealth more difficult. Blockchain transactions require careful onchain and offchain decision-making to avoid transaction overhead.

Immutable Data Privacy Management

Blockchain technology using Ethereum's smart contracts to deliver unhackable, tamper-proof, and immutable data privacy information is the final technological barrier. The eHealth system feeds the smart contract an arbitrary value representing the patient's ultimate decision based on nudge theory. Patients have full control over public access to eHealth data. Patient can function alone.

Some parties allow clear-text data viewing, while others control privacy. The research must address how to integrate this concept in Ethereum's blockchain for smart contracts.

4.CORE SYSTEM COMPONENTS

This section describes our method's main system components. Decentralized e-health, generic nudge theory, and Ethereum-based blockchain-based smart contracts are the core system components. Important Elements of a Blockchain-Based Smart ContractThe primary system components work together to achieve the intended goals, which we employ in Section.

Blockchain's unique features have transformed internet business. Trans operations no longer coordinate parties' goals through intermediaries. Decentralized transaction verification occurs [30]. Blockchain networks distribute ledgers to all nodes. Therefore, all nodes have the same ledger state.

Authorities can validate transaction timestamps and chronological order on a blockchain. Validated and saved data cannot be manipulated, erased, or destroyed by malicious parties. Miners or validators use a consensus mechanism (see Table 2) to validate data transactions, eliminating double entry, faked data, and fraud. Blockchain technology offers decentralization, immutability, security, and transparency.

In 2015, Ethereum platforms popularized smart contract-capable blockchain, nicknamed Blockchain 2.0 (after Bitcoin for Blockchain 1.0). The 2017 update shows that work has continued.

Table 2 Prominent blockchain consensus after the appearance of proofofwork in Bitcoin.

Benchmark	Public Access	Private Access
Distributed Validation	Proof-of-work (PoW), Proof-of-stake (PoS), PoW based derivatives, Federated Byzantines agreement	Proof-of-work (PoW), Proof-of-stake (PoW), PoW based derivatives, Federated Byzantines agreement
Concentrated Validation	Delegated Proof-of-stake (DPoS)	Redundant Byzantine fault tolerance, Rip-ple consensus bilateralnode-to-node (N2N), RAFT and derivatives, Delegated Proof-of-stake (DPoS)

Fig. 1 Proof-of-work consensus has become a popular blockchain consensus mechanism since Bitcoin.

total addresses with balances; zero-balanced addresses are excluded.

Ethereum is a Blockchain 3.0 Initial Coin Offering [32]. Smart contract platforms include Ethereum, Hyper ledger Burrow (Solidity, Serpent, Mutant, and Vipe), Fabric (Golang, Java, JavaScript), Quorum, and Open Transactions.

Smart contracts are confirmed in real time depending on their terms. Since the contract holder can now perform their duties without hindrance, the complicated attestation procedure is abolished. Automating contract functions and integrating operations can speed up corporate services and boost profits. The smart contract-based app improves entity communication. Smart contracts become paperless, cheaper, faster, and more secure with blockchain-level encryption. As seen by the exponential increase of Ethereum addresses (Fig.), smart contracts are widely deployed in many industries and applications due to their benefits. It includes 34,05 million addresses by January 21, 2021. Thus, blockchain-based smart contracts are suited for ehealth, PHI, and EMR.

The Concept of Nudge Theory

The term "behavioural economics" is "nudge theory." Economists adopted psychology's findings to apply them to economics. Traditional economics has shown that theorizing about customer behavior is nonsensical. This notion is based on studying human behavior to determine decision-making causes and effects, not the premise that individuals are intelligent and make reasonable economic judgments.

Western nations have recently tried several approaches to incorporate behavioral economics, notably nudge, into public policy. Behavioral economics, which criticizes mainstream economics' "economic humans" and more plausibly explains human behavior based on psychology, seems appealing at a time when economic incentives, a pragmatic approach to health care policy, are failing.

Nudge strategies utilize financial and non-financial incentives to modify behavior. The nudge technique uses information simplification, physical environment changes, default rules, and social norms as financial tools. This paper will employ the default option to encourage policy subjects to act differently by making the policy makers' chosen options default. Nudge policies that change default settings have been shown to change policy subjects' behavior. Under the idea that "humans tend to select the default option," this option was chosen.

Decentralized EHealth

Ehealth pertains to products and activities that provide routine internet healthcare to individuals or communities. EHealth uses PHI, PHR, and EMR interchangeably to refer to the same duties. These statements have one thing in common: approved users can access their health data on healthcare provider websites. The large number of eHealth providers fragments data and makes it hard for patients to obtain their information, according to [34].

A decentralized healthcare system with different providers is being created using blockchain and smart contracts. Decentralized ehealth was created to organize and improve global healthcare. Table 3 shows standard and decentralized healthcare environments for one and several collaborating servers. Academia and industry have created many methods for time- and location-independent therapies for healthcare professionals, physicians, and patients.

Figure 2 shows blockchain in several applications with different goals. Decentralized value transfer, gamification, openness, interoperability, noncentralized verification, autonomous contracts,

and immutable transactions are the goals. Healthcare use cases include three types:

Table 3 Both centralized and decentralized healthcare have benchmarks.

Benchmark	Architecture	Security
Hierarchical distributed EHR(HDEHR)		N/D
m-Health	DE, P2P	N/D N/D
Ubiquitous PHR (uPHR)		CIA, HIPAA
Conceptual Framework	DE DE	Authentication
(CF)	CS, DOCS	CP-ABE
HealthVaulthealthTicket	CSDC DE	N/D
DEPR	DC	Security
My HealtheVet		Policies
SNOW		Privacy Policies

N/D means undefined, DE means distributed electronic, P2P means peer-to-peer, CS means client-server, DO means distributed object, CIA means confidentiality, integrity, and availability, HIPAA means health insurance protection and accountability, CPABE means ciphertext policy attribute-based encryption, and DC means distributed components

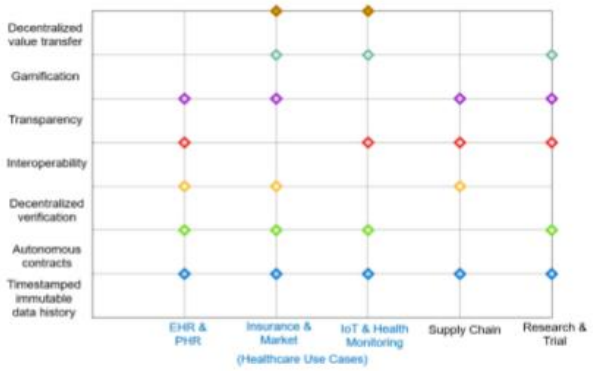

Fig. 2 Blockchain's goal in many use cases [35].

EHR, PHR, market, insurance, IoT, monitoring. Blockchain technology helps some healthcare organizations achieve their goals using various platforms and methodologies [36]. Transparency, value transfer, interoperability, and immutable data historical records are key goals of decentralized ehealth.

5.OPERATINGSYSTEM DESIGN AND IMPLEMENTATION

We'll talk about the operating system and how we'll apply our concepts to help patients select data privacy in decentralized e-health. This paragraph is four-part. We start with cutting-edge PDPM. The work describes data privacy categories and collaborative filtering nudging. Third, the article provides Ethereum smart contract and blockchain-based unchangeable data storage. Finally, complaints are addressed.

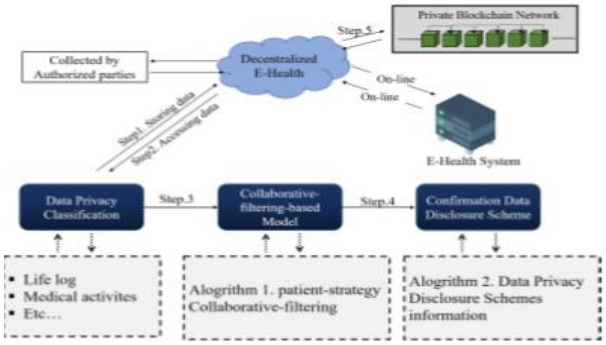

Fig. 3 Our decentralized solution leverages advanced e-health technology.

The State of the Art of PDPM

PDPM reserves patient-defined data in decentralized e-health using "nudges". Inspired by [37], we propose using "nudges" to manage data privacy, classification, and use to improve patient services and suggestions. However, only the patient may set up and control medical information access. Next, an Ethereum smart contract saves nudging output data on the blockchain. Thus, only authorized users can read patient data privacy creations. PDPM uses end-to-end encryption, so only talking eHealth organizations may access messages.

Figure 3 shows the current patient-set data protection PDPM design. Using cloud storage, PDPM initially stores encrypted patient or approved party data. Data is collected by trusted staff, but patients or doctors control access. Because approved doctors or other parties default patient data privacy into lifelong information, medical activities, insurance, etc., the PDPM framework operates.

Collective filtering speeds up PDPM, and patient data classification improves results. Collaborative filtering approach can predict patient privacy and preferences based on PDPM framework recommender system data. The system receives lots of patient and processed data. Joint filtering in PDPM assumes patient X has

Another example illustrates that Patient X agrees with Patient Y more than a random patient. Patient X and Y desire the same use case. The last aspect of the nudge theory suggests that changing the

environment generates automatic cognitive rules that support the desired outcome. Collaborative filtering influences patient behavior.

Data Privacy Classification and Nudging with Collaborative Filtering Model

Internet-stored healthcare data is different and hard to measure. E-health data must be analyzed and merged to improve care. Sharing good eHealth data helps healthcare organizations discuss medical issues, insurance, long-term planning, and more. Filtering the right data before using nudge theory is crucial. This is possible with collaborative filtering.

PDPM's filtering mechanism has two parts. The estimate's goal, active patients, are found by the PDPM.∈ Using ratings from patients with similar symptoms from the first phase, the PDPM predicts the active patient. Patient rating data affects memory-based joint learning models' patient information similarity. Examples include patient-specific topN and neighborhood-based CF. Patient-based methods calculate patient u's item i rating by averaging other patients' ratings. U is the set of the top N patients who rated item i similarly to patient u [38]. Examples of observable aggregation function models

$$r_{u,i} = \frac{1}{N} r_{u^J} i \quad (1)$$

Table 4: healthcare big data.

Data type	Examples
Medical treatment data	EMR, EHR, prescription information, hospitalization and discharging the hospital, medical image data (CT, MRI, CR, etc.)
Clinical research data	Drug clinical trial data, device clinical trial data, genetic study data, human origin study data, survey observation data, research data directly or indirectly using personal information
Public Institution data	Data collected, stored and managed by pub-lic institutions, such as insurance premium- related data, medical treatment details, health examination results, death information, etc.; Medical devices data and patient monitoring device-based data
IoT based data Omics data	Molecular level data like Genome, Transcriptome, Proteome, Metabolome, Epigenome, Lipodome
Lifelog data	Personal record of one's daily life from wearable device (weight, heart rate, blood sugar, personal eating habits, medication, behavior and mental data)
Mobile application and social media data	Various healthcare-related data collected from social media

For the PDPM system is that instead of possessing a high dimensional matrix consisting of abundant missing values, we will deal with a much less matrix in lowerdimensional space. A reduced presentation could be employed for either userbased or itembased neighbourhood algorithms. Like ness computation between items or patients is essential in the PDPM system. Various models, such as Pearson cor relation and vector cosinebased similarity, can be adapted to achieve a better result. Eventually, encrypting the non disclosure patient information can be described as follows:

Input the computed disclosure schemes include the default schemes.

Output is encrypted patient's information.

Check the computed disclosure schemes, if it equals nondisclosure, then go to step 2, otherwise go to step 4.

$$r_{u,i} = k \frac{1}{N} \sum_{u^J \in U} simil(u, u^J) r_{u^J,i} \quad (2)$$

Where k is a normalizing factor defined as k = 1/ u^J U simil(u, u^J). In the PDPM system, we will employ a smaller matrix with fewer dimensions instead of a large matrix with many empty cells. Small displays can be used for user- or item-based neighborhood algorithms. Like-ness computation between objects or patients is key in PDPM. Vector cosine-based similarity and Pearson correlation may boost results. Last, safeguard non-shared patient data:

Projected disclosure methods should incorporate de fault schemes.

Output encryption safeguards subject data.

Continue if estimated disclosure methods match "nondisclosure," step 2. Different? Go to step 4.

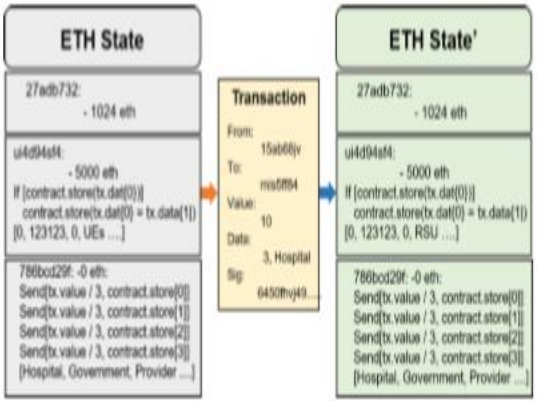

Fig. 4 State transition function in the Ethereum transaction.

To store the latest nudging-generated personal patient data, use an Ethereum smart contract with collaborative filtering. Only authorized users can see eHealth system events on a private Ethereum blockchain. Data can be used for AI technology analysis, insurance proposals, therapy

descriptions, and more by doctors and stakeholders.Ethereum transfers are powered by the EVM, the protocol's brain. Fig. shows EVM. 1, uses stacks and state transactions differently. 4. Sorts all memory numbers. The EVM protects transactions with elliptic curve and naive hashing and a 256-bit word size. These data components are accessible in the EVM:

Ethereum uses ROM for permanent storage. It contains executable bytecode for any-value methods.

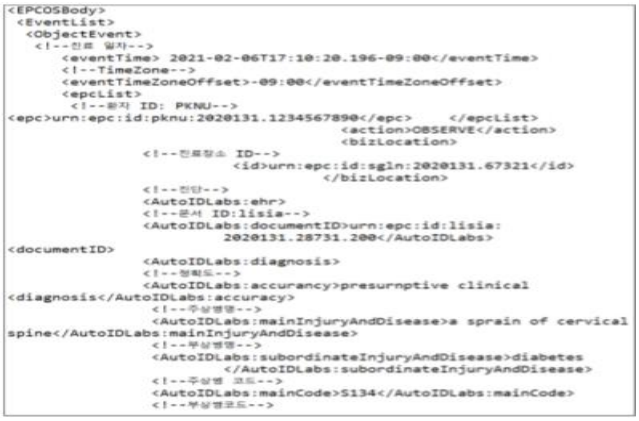

Fig. 5 A visible temporary memory that zeros areas.

The clinical EHR data style (Fig. 5) is utilized to insert values into smart contracts to simplify things. After choosing private and public data, the patient chooses the EHR style. Different autonomous e-health systems maintain private patient data differently, as seen in Tables 1 and 3. Random data is supplied into the smart contract, which saves and publishes it. We create Ethereum smart contracts with GanacheTruffle. This enables us experiment, follow directions, and monitor blockchain transactions (blocks, transactions, and logs).The Ganache GUI generates eHealth entity account addresses from the public address and secret key. Ganache Lever aged Ethereum Js to simulate client commands. The usual Ganache configuration is operating on an RPC server at HTTP://127.0.0.1:7545 with the network ID 5777 in "Automining" mode. Ganache GUI automatically handles each entity's Ether (100.00 ETH), gas prices (20000000000), and gas limitations (6721975). MetaMask (metamask.io) is a crypto wallet and gateway to a decentralized ehealth application that helps entities manage wallets.Electronic health records are employed in therapeutic operations. We got the construction plan from [40].

Figure 6 shows how the blockchain network tracks patients who utilize smart contracts on their devices to perform e-health deals. We split the e-health entity into hospital (Hs A), which owns the smart contract, patient A (Px A), and patient B (Px B). The first transaction was recorded. It was a blockchain contract migration transaction so everyone could use Hs A's contract. Each relocated smart contract has a unique identifier to distinguish it from other blockchain contracts.

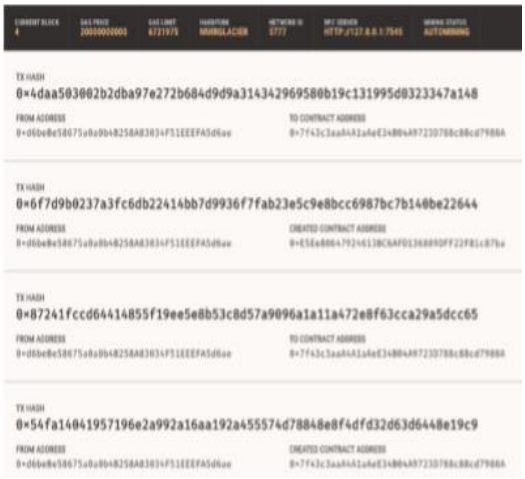

Fig. 6 Smart contract migration in e-health.

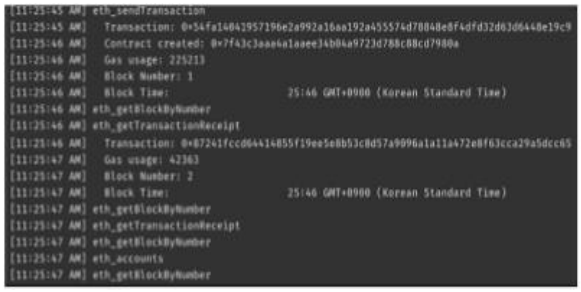

Fig. 7 Manage patient business.

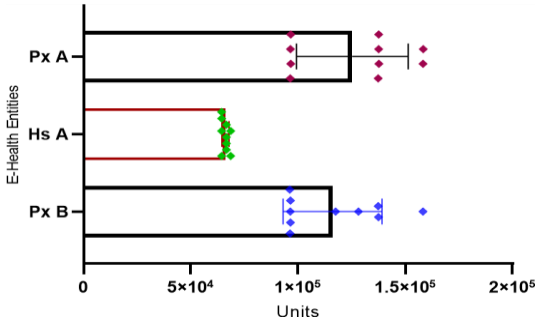

Fig. 8 Hospital's estimated Ether spend.

Figure 1 lists all deals. 8. We tracked gas use for Px A, Px B, and Hs A. The number of random inputs and outputs were similar for Px A and Px B. The initial exchange showed that Px A needed 96371 units of gas to adjust the settings based on its information. The last transaction used 158426 units, with an average of 125309 units. Px B's

transactions are similar to Px A's. Until Tx10th, which averaged 66141 units, the initial transaction consumed the least gas, 96208 units. Different eHealth data formats used as smart contract inputs are essential.

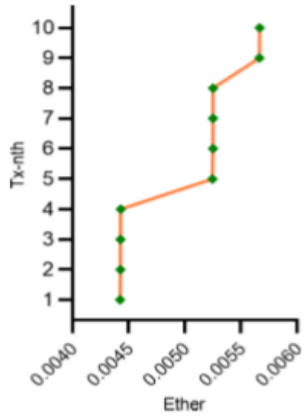

Fig. 9 Patients received coin incentives as depicted

Ether is used. For optimal data management, patients receive cryptocurrency. Patients also improve the PDPM system. Benefits vary by contribution. The system provider or smart contract owner controls incentive policies. As long as the owner doesn't cancel, the arrangement will continue. Ethereum smart contracts generally support PDPM. We need an easy-to-use, effective smart contract to reduce e-health transaction expenses.

Concerns and Remarks

PDPM protects patient data in decentralized e-health environments using nudge theory. We discussed the benefits of PDPM in e-health before. However, our strategy affects technical and theoretical issues and is linked to other issues.

LargeScale Medical Data

The PDPM system requires a lot of e-health data from patients, stakeholders, and other organizations in various areas. However, collaborative filtering works well with enough user and healthcare stakeholder data. As a fresh suggestion system, the PDPM system can be difficult to start since it lacks data. It's hard to predict new user patterns before testing filters. Collaborative filtering and nudging algorithms employ integrated data to give patients the best data privacy recommendations. By adding cheaper monitors and devices to the internet of things, healthcare could improve data collection. A suitable model that can handle different sensor devices and data types is needed to gather sensor data. Sensor data must be collected before creating environmental data. We believe our data collection methods are safe for this study even without a process. The PDPM system needs fast, stable, and safe data collecting to meet targets soon..

Nudging Data and Collaborative Filtering

Implementation of the nudge plan is likewise problematic. Ethics and personal choice must be considered while using nudging in e-healthcare. Nudge treatments are supposed to impact automatic systems, so changing someone's behavior may be too much work for medical professionals or system designers and manipulative. Thus, nudges can alter behavior in modest ways. Sometimes prejudice is used to achieve policy aims, and sometimes it is fixed to help the policymaker make the proper choice. Nudge policymakers can't be entirely objective. They can't guarantee that nudge policies will improve decision-making and self-esteem. In the end, it's hard to grasp how imperfect people's rules might affect their behavior. It also contradicts the RCTs that inspired the nudging strategy.

Transparency Concerns

One of blockchain's biggest benefits is transparency. Exchanges occur on the public blockchain, which anybody can observe. Openness characterizes SC blockchain. Sometimes this feature is bad, such with private PDPM data. Anonymous digital asset owners' addresses can be seen by the public without logging in. This function shows where cryptocurrency comes from and is spent in the blockchain. This eliminates transaction confusion. Transparent deals aren't always good. For instance, handling sensitive and confidential data, like in most e-health contexts, is bad. Before using blockchain in the PDPM system, more research on transparency data in decentralized e-health is needed, as mentioned in and.

Scalability Issues

PDPM tracks patients' data privacy decisions using Ethereum smart contracts. Ethereum's use has unfixable issues. Ethereum miners compete to

find the target-difficult nonce. Each node must also verify the miner's work and store the network's current status. Ethereum transaction speed is greatly reduced by this technique. Transactions per second are limited to 1215. Increasing block size and consensus difficulty to solve scaling issues compromises blockchain security and independence. The "blockchain scalability trilemma." impacts health care facilities. The procedure in [45] can alleviate these concerns. Overhead and bottlenecks can be avoided by accurately estimating patient numbers and data.

6.CONCLUSIONS

We created the PDPM to provide patients choice over their data privacy in autonomous e-health environments utilizing incentive theory. We want to construct a cutting-edge PDPM that leverages nudge theory and blockchain technology to protect patients' data in e-health systems. The PDPM system we created is the first step toward our plan. This study reviews the merits and downsides of using many technologies to help the PDPM achieve its goals. The PDPM system will use Ethereum smart contracts for persistent data privacy management. Because of their minimal transaction costs and superior services. The blockchain scalability trilemma must be examined to discover a balance between security, decentralization, and scalability. We need to know how many entities are in the PDPM system for future development. In fact, our next project will push real patient data with a collaborative filtering system and improve the Ethereum smart contract by decreasing random inputs.

REFERENCES

1. R. Kumar, W. Wang, J. Kumar, T. Yang, A. Khan, W. Ali, and I. Ali, “An integration of blockchain and ai for secure data sharing and detection of ct images for the hospitals,” Computerized Medical Imaging and Graphics, vol.87, p.101812, 2021.
2. S. Becher, A. Gerl, B. Meier, and F. Bölz, “Big picture on privacy en hancing technologies in ehealth: a holistic personal privacy work flow,” Information, vol.11, no.7, p.356, 2020.
3. Y. Hong, T.B. Patrick, and R. Gillis, “Protection of patient’s privacy and data security in ehealth services,” 2008 international confer ence on biomedical engineering and informatics, vol.1, pp.643–647, IEEE, 2008.
4. C. Butpheng, K.H. Yeh, and H. Xiong, “Security and privacy in iotcloudbased ehealth systems—a comprehensive review,” Sym metry, vol.12, no.7, p.1191, 2020.
5. Roehrs, C.A. Da Costa, and R. da Rosa Righi, “Omniphr: A distributed architecture model to integrate personal health records,” Journal of biomedical informatics, vol.71, pp.70–81, 2017.
6. DICOM, “Digital imaging and communications in medicine,” https://www.dicomstandard.org/, 2021.
7. J.C. Mandel, D.A. Kreda, K.D. Mandl, I.S. Kohane, and R.B. Ramoni, “Smart on fhir: a standardsbased, interoperable apps plat form for electronic health records,” Journal of the American Medical Informatics Association, vol.23, no.5, pp.899–908, 2016.
8. S. Rahmadika and K.H. Rhee, “Blockchain technology for provid ing an architecture model of decentralized personal health informa tion,” International Journal of Engineering Business Management, vol.10, p.1847979018790589, 2018.
9. G. Tripathi, M.A. Ahad, and S. Paiva, “S2hsa blockchain based approach for smart healthcare system,” Healthcare, vol.8, no.1, p.100391, Elsevier, 2020.
10. M.M.H. Onik, S. Aich, J. Yang, C.S. Kim, and H.C. Kim, “Blockchain in healthcare: Challenges and solutions,” Big data ana lytics for intelligent healthcare management, pp.197–226, Elsevier, 2019.