Blockchain: Research and Applications 6 (2025) 100242

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

Research Article

SSI-MedRx: A fraud-resilient healthcare system based on blockchain and SSI

Meriem Guerar [a,*], Mauro Migliardi [b], Enrico Russo [a], Djamel Khadraoui [c], Alessio Merlo [d]

[a] DIBRIS, University of Genoa, Genova 16146, Italy
[b] UNIPD, University of Padova, Padova 35131, Italy
[c] Luxembourg Institute of Science and Technology (LIST), Esch-sur-Alzette L-4362, Luxembourg
[d] School of Advanced Defense Studies, CASD, Rome 00165, Italy

ARTICLE INFO

Keywords:
Self-sovereign identity
SSI-based authentication
Fraud
Security & privacy
Blockchain
Healthcare
Patient-centric

ABSTRACT

Today, healthcare fraud poses a significant issue, encompassing everything from falsified billing claims and phantom services to the excessive prescription of opioid medications and medical identity theft. These deceptive activities cause substantial financial losses, erode patient trust, compromise healthcare quality, and threaten patient safety. In this paper, we introduce SSI-MedRx, a healthcare system based on blockchain technology and Self-Sovereign Identity (SSI). It is designed to ensure cross-border interoperability, preserve patient privacy, and prevent challenging healthcare frauds, including medical identity theft, phantom billing, kickbacks, and opioid overprescribing. By design, our system empowers patients by granting them complete control over their personal and health data. This shift toward patient-centric data management can potentially reduce the risk of data breaches, enhance care coordination, and improve overall healthcare outcomes.

1. Introduction

The current healthcare system relies on centralized structures to manage patient data within individual healthcare institutions, often resulting in fragmented and disconnected data systems. This fragmentation leads to significant challenges, such as transferring patient data between various healthcare institutions. One of the critical issues is interoperability, as different healthcare systems might use incompatible data formats and standards. This lack of interoperability hinders the seamless exchange of patient data, creating delays in care, miscommunication, and increased costs. In addition, centralized systems can pose security and privacy concerns, especially when sharing sensitive patient information. These concerns become particularly evident when data breaches occur, putting patient confidentiality at risk. Each data breach can compromise patient records, leading to potential identity theft and fraudulent activities in the healthcare sector, such as phantom billing [1]. Phantom billing is a dishonest practice in the healthcare industry, where healthcare providers or entities submit false claims for medical services or procedures which are never performed or provided to patients. This deceptive billing scheme often results in financial gain for the fraudulent entity, as they receive payments or reimbursements from insurance companies for services that never occurred. In addition to phantom billing, healthcare fraud encompasses other harmful practices that endanger patient well-being. Two prominent examples are kickbacks [2] and opioid overprescribing [3]. Kickbacks involve healthcare professionals who receive improper financial incentives or other incentives in exchange for patient referrals or the promotion of specific medical treatments. Such practices can undermine the objectivity of medical decisions, potentially leading to unnecessary treatments, medications, or procedures that jeopardize patient health [2]. Opioid overprescribing, refers to the excessive prescription of opioid medications, exposing patients to a higher risk of opioid dependence, addiction, overdose, and related health problems. These fraudulent activities underscore the need for secure and decentralized healthcare systems prioritizing patient safety and privacy.

The unique features of blockchain technology, particularly the public blockchain, such as data immutability, transparency, and decentralized consensus mechanisms, can be leveraged to address certain types of frauds effectively. For instance, blockchain technology has recently demonstrated its effectiveness in combating frauds in the fi-

* Corresponding author.
E-mail addresses: meriem.guerar@unige.it (M. Guerar), mauro.migliardi@unipd.it (M. Migliardi), enrico.russo@unige.it (E. Russo), djamel.khadraoui@list.lu (D. Khadraoui), alessio.merlo@ssuos.difesa.it (A. Merlo).

https://doi.org/10.1016/j.bcra.2024.100242
Received 2 January 2024; Received in revised form 11 October 2024; Accepted 13 October 2024
Available online 13 December 2024
2096-7209/© 2024 THE AUTHORS. Published by Elsevier B.V. on behalf of Zhejiang University Press. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

nancial sector [4,5] and mitigating the spread of fake news on social media [6]. However, integrating blockchain technology into healthcare systems is challenging due to the trade-off between transparency and maintaining patient data confidentiality. In response to this challenge, some researchers have opted for private permissioned blockchains [7–9], albeit at the cost of limiting the healthcare system's borderless capabilities.

In contrast, our proposed solution, SSI-MedRx, leverages a public blockchain to store non-confidential data necessary to prevent phantom billing frauds. Meanwhile, the patient's personal and health data are stored on their own devices. Thanks to the self-sovereign identity model, SSI-MedRx puts patients at the center of their healthcare journey, fostering a patient-centric approach. It empowers them to engage more proactively in their health condition and decide what information to share, with whom, and when. Furthermore, having all patient data stored in their SSI-MedRx wallets enables us to integrate countermeasures against opioid overprescribing without compromising patient privacy. The SSI-MedRx wallet in the patient's device is designed to identify and decline new prescriptions if the prescribed medications, when combined with a patient's current treatments, pose a risk of addiction. In addition, SSI-MedRx offers cross-border interoperability between the different healthcare institutions by design.

2. Healthcare system and threat model

The healthcare system offers a variety of services. This paper will primarily focus on two essential services, e-prescriptions and insurance, as they are frequently associated with common healthcare fraud scenarios [2].

According to a recent study [10], many e-prescription systems operate centrally, especially in Europe. Once doctors issue prescriptions, they are stored in the system and instantly accessible across all pharmacies upon request. Doctors then provide a token or a unique code in the form of a QR code to the patients, which can be scanned by the pharmacists to access the prescription. Before dispensing the medications, the pharmacists will check the patients' identity by verifying their ID cards and subsequently update the prescription status in the centralized database. For prescriptions that need to be renewed regularly, patients can contact the doctor via email or phone and collect the medicine from the pharmacy without visiting the doctor in person. Although e-prescription and healthcare systems offer numerous advantages over paper-based systems, they are still susceptible to certain types of frauds, security vulnerabilities, and privacy concerns.

2.1. Medical identity theft

Medical identity theft, with an annual cost of over $30 billion to the healthcare industry [11], involves the illegal use of individuals' personal information, such as their name, social security number, or health insurance details, to receive medical treatment, fill prescriptions, or obtain health services. A Ponemon Institute study [2,12] found that 65% of victims had to pay an average of $13,500 to resolve the issue, often reimbursing healthcare providers or insurers for fraudulent services or seeking assistance from identity service providers or legal counsel to determine the incident and prevent future fraud. This type of fraud can occur through outsiders and insiders within healthcare providers. The consequences of medical identity theft can be severe, leading to financial losses, incorrect medical records, delayed or improper medical treatment, stolen benefits, and even criminal charges.

2.2. Phantom billing

Annually, medical insurance funds worldwide cause an approximate loss of $260 billion [13]. In 2016, more than 300 individuals, including doctors, nurses, and pharmacists, faced charges related to healthcare fraud schemes, amounting to $900 million in false billings [14]. In this section, we present one of the most common types of fraud, phantom billing [1], which is particularly challenging to detect. This fraudulent activity often involves collusion between doctors and pharmacists, where they submit false bills to obtain reimbursements for drugs that were never dispensed. These illicit drugs may later reach the black market or dark web, perpetuating the fraud cycle. The process usually includes the unauthorized use of a patient's personal and insurance information in deceptive claims. As a result, patients may unknowingly become victims of medical identity theft, particularly members of vulnerable groups such as the elderly who may have chronic health conditions, limited technology proficiency, and are often less vigilant in monitoring their accounts through web portals. Besides, the difficulty of gathering evidence and the fear of consequences may deter victims from speaking up about such fraudulent practices. Unfortunately, the existing e-healthcare systems lack adequate measures to prevent such fraud. They rely heavily on trust and do not require patients' consent to access their data, leaving room for certain unethical service providers to exploit this vulnerability to profit from the insurance reimbursements.

2.3. Kickbacks

Kickbacks are illegal payments or other advantages provided by pharmaceutical companies to medical professionals or individual pharmacists as an incentive for promoting specific drugs. This illicit practice can compromise a medical provider's decision-making, prioritizing profit over the patient's well-being which should be the primary goal of healthcare providers [2]. In 2016, ProPublica [15] conducted a study on the 50 most-prescribed brand-name drugs, revealing a consistent correlation between doctor payments and prescription rates. For example, doctors who received payments related to Linzess, a drug for severe constipation and irritable bowel syndrome, wrote 45% more prescriptions for it compared to those who did not receive payments. This trend was not limited to Linzess; similar patterns were observed for drugs, such as Mybetriq and Restasis, where higher prescription rates were associated with payments from the respective pharmaceutical companies. The study identified this trend in 46 out of the 50 drugs studied.

2.4. Opioid overprescribing

The overprescription of opioids, fueled by deceptive marketing practices by pharmaceutical companies, has been a significant contributing factor to the current opioid crisis [3]. Misleading campaigns have downplayed the risks of addiction and exaggerated the benefits of pain relief, leading healthcare providers to believe that opioids are a safe and effective solution for a wide range of pain conditions [3]. Additionally, pharmaceutical companies offered kickbacks to healthcare providers, creating conflicts of interest and potentially leading to unnecessary prescriptions of opioids [16]. As a consequence, there has been a significant increase in addiction, overdose deaths, and burden on healthcare systems [16]. From 1999 to 2021, opioid overdose caused over one million deaths in the US [17]. To tackle this critical issue, prescription drug monitoring programs (PDMPs) have been implemented to track controlled substance prescriptions. However, the existing PDMPs face various limitations, including lack of interoperability and data sharing across states, the vulnerability of centralized databases, inadequate identity verification, and reliability and consistency issues [18]. Additionally, the fact that PDMP usage is optional leads many physicians to neglect to check their patients' drug consumption history before prescribing medications, making it difficult to reduce drug abuse incidents significantly [19].

2.5. Data breaches

Although centralized healthcare systems offer several advantages regarding information accessibility and ease of use, they also have potential vulnerabilities. The fact that they represent a single point of failure makes them susceptible to cyberattacks, putting patient privacy at risk and potentially leading to significant data breaches, as recent events in Ireland demonstrated. In May 2021, Ireland's Health Service Executive (HSE) suffered a major ransomware cyberattack [20]. Cybercriminals infiltrated its centralized systems, stealing many patients' personal information. Then, they asked for a ransom for the non-publication of stolen data and provided a tool to restore access to the encrypted data. The cyberattack led to a suspension of the majority of its IT systems, causing delays in providing treatments and significant disruption to healthcare services across the country during the COVID-19 pandemic [20]. In February 2022, another cyberattack took place, affecting 345,000 individuals [21]. The attackers illicitly accessed ARcare's computer systems, obtaining sensitive personal data such as names, social security numbers, driver's license numbers, dates of birth, financial account details, prescription information, medical diagnoses, and health insurance data. After the breach, specific stolen data were made public on the internet.

2.6. Privacy concern

Medical health records and prescriptions contain sensitive information about the patients and their health conditions, such as prescribed medications, dosage instructions, and other relevant medical details. Unfortunately, the centralized databases where these data are usually stored are susceptible to data breaches and unauthorized access, posing significant privacy risks. For instance, PillPack collaborated with ReMyHealth to access patient data collected by SureScripts, an e-prescription management system in the USA. However, in 2019, it was discovered that ReMyHealth was involved in fraudulent activities, providing unauthorized access to patient health information and exploiting prescription data for marketing purposes [22]. This breach of privacy can lead to potential misuse of the information, cause emotional distress for the patients, and potentially harm their personal and professional lives. Therefore, safeguarding these data from unauthorized access is crucial to ensure patient privacy and maintain confidentiality.

3. Overview of the proposed system

3.1. Requirements specification and guideline

To develop a healthcare system that is resilient against the abovementioned frauds with respect to privacy and operates without geographical constraints, it is crucial to consider the following critical requirements during the design phase: security, privacy, fraud-resilience, interoperability, and borderlessness.

3.1.1. Security

This section discusses the security features that should be considered when addressing medical identity theft and data breaches.

- Robust authentication: It is essential to implement a robust authentication method to prevent unauthorized access to the system. Conventional centralized or federated authentication methods are well-known for their susceptibility to data breaches and cyberattacks. Although researchers have dedicated significant efforts to enhancing the security of PINs and passwords [23–28], given their widespread adoption and familiarity, their proposed solutions primarily focus on addressing client-side attacks, leaving the server-side susceptible to data breaches. Therefore, adopting a user-centric approach, such as SSI-based authentication methods where users have control over their digital identities, is highly recommended.

- No single point of failure: Centralized healthcare systems represent a single point of failure, rendering them more susceptible to data breaches and theft. Therefore, it is essential to consider adopting a decentralized and user-centric approach.

- Secure data exchange: Within specific healthcare systems, medical data are transferred among various healthcare providers or institutions via emails or insecure channels [9]. Thus, employing a secure communication channel that guarantees the confidentiality, integrity, and authenticity of messages shared between these parties is essential.

- Full control and ownership: Users should have complete control and ownership of their health data and keys. Using edge wallets, users' data are stored locally on their devices. Thus, users own and have complete control over their keys and data, reducing the system's attractiveness as a target and making it more challenging for attackers to compromise a large dataset all at once. On the other hand, a cloud-based wallet requires a high level of trust in the cloud service provider to protect both the data and the encryption keys. Typically, the vendor has total control over the user's key; thus, it is not self-sovereign.

- Public verifiability and authenticity: Public verifiability means that anyone, without the need for special access or privileges, can independently and transparently verify the authenticity and accuracy of the data. On the other hand, authenticity focuses on confirming that the data are genuine, unaltered, and trustworthy, which is crucial in a healthcare system. Taking a prescription as an example, the healthcare system should allow any pharmacy to verify the authenticity of the prescription, ensuring that it has not been tampered with, the doctor is authorized to prescribe the medication, and the patient is eligible to receive the medication and benefit from insurance. In SSI-based healthcare systems, achieving these goals involves utilizing cryptographic signatures and public blockchains, or similar solutions.

3.1.2. Privacy

The healthcare system must guarantee the confidentiality of patients' personal and health data to comply with regulations, such as the General Data Protection Regulation (GDPR). Storing these sensitive data off-chain is highly recommended.

- Data confidentiality: The healthcare system should ensure that patients' personal and health data are kept confidential by securely storing data and preventing unauthorized access or disclosure.

- Auditable consent: Patients must explicitly approve the access and sharing of their personal and health data in a way that allows for subsequent auditing or verification. They should be able to decide which data to disclose, to whom, and for what purpose. This control reduces the risk of unauthorized data access and mitigates the chance of data misuse.

3.1.3. Resilience to healthcare frauds

- Phantom billing: The healthcare system needs to provide mechanisms that allow insurance providers to 1) confirm the authenticity of a prescription, 2) ensure that patient data are used with explicit consent, and 3) verify that the prescription is indeed dispensed.

- Kickbacks The healthcare system should enable doctors to prescribe medication only using the medication's active ingredient, which describes the primary chemical compound in the medicine, rather than relying on the brand name. Embracing this practice could lead to various advantages, such as reducing medication errors for doctors and patients and mitigating the risk of kickback fraud associated with doctors who receive payments. In addition, patients should be free to choose between purchasing the generic or brand-name drug, considering factors, such as price, the reputation of the drug, or their personal preferences.

- Opioid overprescribing: The healthcare system should implement effective countermeasures against opioid overprescribing while ensuring that patient privacy is not compromised.

3.1.4. Interoperability

Interoperability in healthcare often involves adhering to standardized data formats and communication protocols to facilitate the exchange of patient data. In healthcare systems based on SSI, data are shared through Verifiable Credentials (VCs) or Verifiable Presentations (VPs). Thus, to ensure interoperability, it is crucial to 1) define technologies and standards that enable VC issuance and presentation, verification, and exchange to ensure that different healthcare entities can effectively communicate using a shared framework, 2) define credential schema to ensure that the semantics of the data within the VC remain consistent and are correctly understood by different healthcare entities, promoting semantic interoperability, and 3) use standardized data formats such as JSON for Linked Data (JSON-LD) or JSON Web Tokens (JWT). These formats enable healthcare entities to understand how data are structured and encoded within VCs, promoting syntactical interoperability.

3.1.5. Borderlessness

The system should enable any verifier to check the validity and authenticity of the data the holder shares, regardless of their geographical locations. For example, patients should be able to fill their prescriptions regardless of location. Governance frameworks covering legal and technical aspects play a crucial role in creating borderless SSI-based systems. This requirement has strong implications for international regulations and legislation. However, avoiding making the technology an additional hurdle to overcome is essential.

3.2. SSI-MedRx overview

Following the critical requirements defined above, we developed SSI-MedRx. This universal privacy-preserving healthcare system focuses on e-prescription and insurance services while addressing prevalent fraud issues, such as phantom billing, kickbacks, opioid overprescribing, and medical identity theft. The system allows physicians to prescribe medications, pharmacies to dispense them and ask for refunds, patients to own, control, and manage their prescriptions and health records, and insurance providers to verify the process and reimburse pharmacies.

Unlike in the existing healthcare systems, the patient's information, health records, and prescriptions are stored neither in a centralized database nor on the blockchain; instead, they are stored in the form of verifiable credentials within the SSI-MedRx wallet on the patient's devices and securely shared off-chain through OpenID for Verifiable Credentials (OID4VC) [29]. In this way, patients will have complete control over their personal and health data, enabling them to share these data privately with whom they want and when they want. A lifetime patient prescription history on the patient device allows the system to enforce rules to protect their safety without compromising privacy. For instance, the system can automatically check the opioid drugs recently taken by the patients, allowing it to approve or reject the new prescription issued by the physician based on a permissible dosage that prevents any risk of addiction. The concept revolves around not solely relying on the trust of physicians, as they might have ethical or competency issues. Instead, the approach is to "trust but verify", ensuring patient safety without putting the patient's medical history in a centralized database accessible by all healthcare service providers, regardless of their involvement in the patients' care. According to Ref. [30], the basic design of most e-prescription systems varies slightly. However, significant differences arise in the authentication procedure, posing a considerable challenge in achieving cross-border interoperability, which is currently limited. Therefore, we opt for a self-sovereign identity model to authenticate healthcare professionals and exchange confidential data. Under the guidance outlined in section 3.1.4, SSI-MedRx can guarantee cross-border accessibility and interoperability of healthcare professional cards used for authentication, as well as other exchanged data such as prescriptions, health records, and invoices. In addition, we use edge wallet to store users' keys and health data, which substantially decreases the risk of data breaches linked to centralized data storage and reduces identity theft. Stealing user's information would not be enough to impersonate them, moreover, attackers would need to possess their corresponding keys stored in their mobile devices in a secure storage such as Secure Element (SE). Furthermore, SSI-MedRx leverages blockchain technology to track medicines' prescription status and payment transactions in MedRx tokens. These ERC20 tokens can be purchased through the platform in exchange for fiat, 1 dollar for 1 MedRx token. Tracking payment through blockchain serves as proof of prescription dispensation and aids insurance companies in preventing reimbursement for phantom billing.

3.3. Involved actors

Our system's main entities include governance authority, government/insurance, healthcare authority, patient, doctor, and pharmacy.

Governance authority: The governance authority is a global entity or consortium of organizations responsible for creating and administering the governance framework. This framework is a set of business, legal, and technical rules that can be enforced through law and computer code. It serves the dual purpose of facilitating fraud prevention and fostering interoperable digital trust ecosystems adaptable to diverse sizes and scopes. For instance, through the governance framework, the governance authority creates trust between verifiers and issuers who might not know each other by defining a trusted issuer registry.

Government/Insurance: In various healthcare systems worldwide, the responsibility for issuing identity cards and insurance cards may fall on one or two distinct entities, depending on the specific structure of each country's healthcare system. For instance, in Italy, the government assumes the role of both the insurer and the identity card issuer, providing Italian citizens with the national health card, known as the "Tessera Sanitaria", granting them access to a range of healthcare services. In the context of this paper, the functions of government and insurance, whether public or private, are unified under a single entity. This entity is responsible for issuing identity and insurance cards VCs to citizens. It verifies prescription VPs and invoices VCs submitted by pharmacies for reimbursement. In the following sections, the specific name for this entity will be chosen based on the service being discussed.

Healthcare authority: This authority might have different names and structures depending on the country. It is worth mentioning that the structure does not impact the functioning of our system. From our point of view, this authority's primary role is to issue verifiable ID cards to healthcare service providers attesting to their healthcare professional status.

Doctor: Doctors are responsible for diagnosing patients, verifying their identities, and issuing prescriptions in the form of VC.

Patient: A patient is typically a citizen seeking medical treatment and holding VCs in their SSI-MedRx wallets. The patient can present proofs of claims from one or more credentials when requested by the verifiers. For example, patients present their VC card identification to a doctor and a pharmacy to prove their identity and their VC insurance to prove that they are covered by insurance.

Pharmacy: It is the entity that administers prescriptions. It takes on the role of a verifier when the patient is requested to present their identity card, prescription, and insurance card VCs, as well as the role of an issuer when it issues the invoice VC and a refund request VC.

3.4. SSI-MedRx ecosystem and trust model

As shown in Fig. 1, the SSI-MedRx ecosystem includes four components to ensure cross-border accessibility, seamless interoperability, and trust among stakeholders.

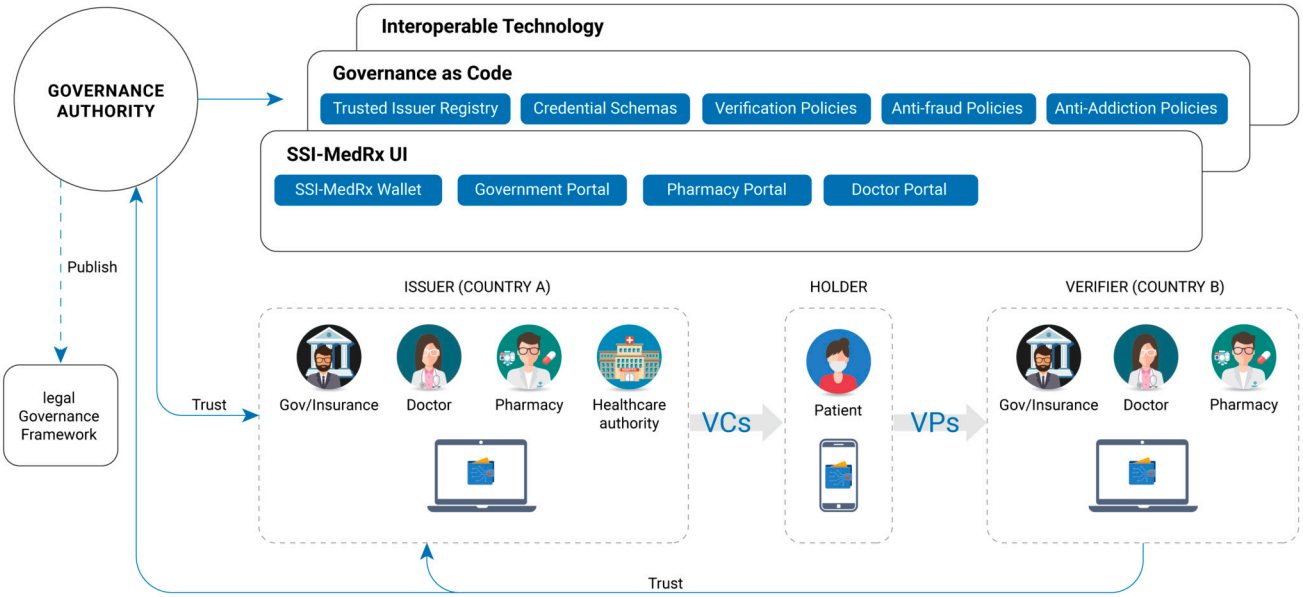

Fig. 1. SSI-MedRx ecosystem and trust model.

3.4.1. Interoperable technologies

This first component defines the SSI technology stack on which SSI-MedRex is built. The governance authority selects different technologies and standards, including decisions on the data model and format, Decentralized Identifier Methods (DIDs), data exchange protocols, etc.

3.4.2. Governance as code

This component specifies rules enforced programmatically by the governance authority. This includes trusted issuer registries, credential templates or schemas, verification policies, anti-fraud policies, and anti-addiction policies. A trusted issuer registry should be stored on a public blockchain and is used to list issuers that can be trusted. In scenarios involving multiple countries utilizing the system, the governance authority can add only the governments to the trusted issuer registry and grant them authorization to accredit other trusted issuers in their corresponding countries, such as doctors and pharmacies, to issue certain types of VC. Credential templates are used to define the attributes that each verifiable credential type should include. Storing these templates on the public blockchain ensures semantic interoperability. Verification policies define the requirements for a successful VP verification. In SSI-MedRx, we use the following policies to verify the VP:

1) Signature policy: it verifies the cryptographic signature of the credential to ensure its integrity and authenticity.

2) JSON schema policy: it checks that the verifiable credential content matches their specific credential template or schema.

3) Challenge policy: it validates that the presentation is signed with the challenge (i.e., nonce) requested by the verifier backend to prevent replay attacks.

4) Presentation definition policy: it verifies that the received verifiable presentation meets the verifier's expectations and provides the required proofs and inputs, as specified in the presentation definition included in the authorization request. The governance authority should define the presentation, and one advantage of this is that it prevents verifiers from requesting or obtaining information beyond what is explicitly defined and permitted by the governance authority.

5) Role policy: this policy verifies whether the healthcare professionals' role authorizes them to access a specific SSI-MedRx portal as specified on the credential. Unlike the other verification policies, this policy only verifies healthcare professional ID VC.

On the other hand, anti-fraud policies constitute a set of rules enforced through the SSI-MedRx smart contract to prevent phantom billing fraud. Anti-addiction policies are a set of rules enforced by the SSI-MedRx wallet to ensure patient safety against opioid addiction or overdose death.

3.4.3. SSI-MedRx UI

This component provides a mobile or web portal for stakeholders to interact with the SSI-MedRx system.

3.4.4. Legal governance framework

A legal governance framework consists of a set of legal rules published by the governance authority. A complete set of international agreements must be fully operational to ensure a borderless structure.

Thanks to the governance framework, VCs can scale and function effectively within trust communities of any size, ranging from a single state to multiple countries. In SSI-MedRx's trust model, the verifiers trust the governance authority and issuers registered in the trusted issuer registry, which is recorded in the public or public permissioned blockchain. Thus, if the patient receives a prescription VC from a doctor in country A, he/she can easily redeem it in country B. Before dispensing the prescription, the pharmacy can verify the prescription VP according to verification policies defined by the governance authority and prescription status through the blockchain.

3.5. SSI-MedRx process workflow

Figs. 2 and 3 illustrate the authentication of healthcare providers, the primary SSI-MedRx process, and the interactions between stakeholders and the smart contract SSI-MedRx.

1) Healthcare professionals' authentication to SSI-MedRx: Once the doctors and pharmacies are registered with the trusted issuer registry, they can issue certain VCs. Nevertheless, they must log to the SSI-MedRx platform through their healthcare professional ID VC issued by the healthcare authority (see Fig. 2). SSI-MedRx verifies the healthcare professional roles, VC schemas, challenges, and presentation definitions. In addition, it resolves the healthcare authority's DID to look up the public key in the DID document needed to verify the VC signature.

2) Patient identity verification and prescription issuance by the doctor: When patients visit a doctor, they present their identity card (Step 2.1), a government-issued VC. The doctor portal automatically verifies the VP according to the verification policies defined above, such as whether the VC matches the format specified in the credential template

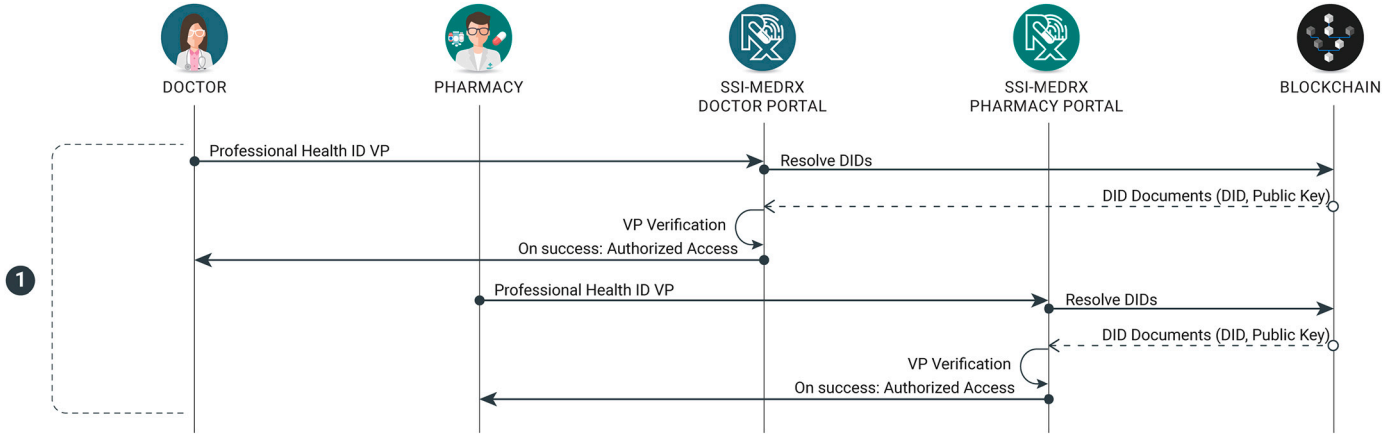

Fig. 2. Healthcare professionals authentication to SSI-MedRx workflow.

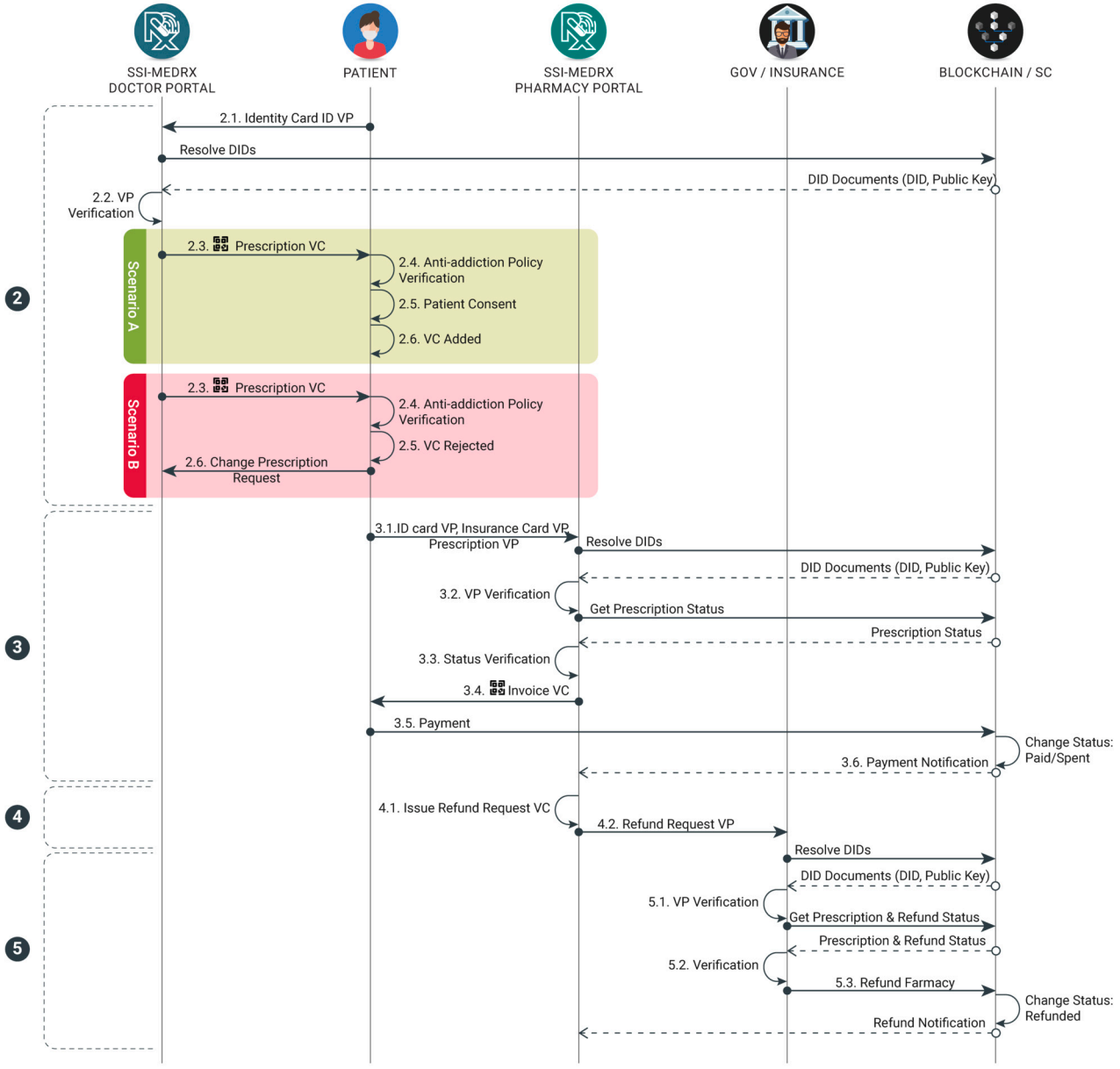

Fig. 3. SSI-MedRx process workflow.

and whether a trusted issuer has signed it. If the verification in Step 2.2 is successful, the prescription form is generated with pre-filled patient and doctor information. The doctor must complete the prescription by adding the necessary medications and issuing the VC. The patient can obtain this VC through a simple QR code scan using their SSI-MedRx wallet (Step 2.3). Before asking the patient to accept the VC, the wallet verifies whether the prescribed medications, when combined with any other treatments the patient is undergoing, exceed the permissible dosage of substances that could potentially lead to addiction (Step 2.4). Only when the prescription meets these criteria can it be added to the patient's wallet (i.e., Fig. 3, scenario A, Step 2.6). Otherwise, as shown in Fig. 3 scenario B, the wallet rejects the prescription VC (Step 2.5) and notifies the doctor (Step 2.6) who can then suggest an alternative treatment. The patient is free to share further information with the doctor.

3) Patients' VCs verification and payment process at the pharmacy: The patient goes to the pharmacy and presents his/her identity card, prescription VCs, and insurance card VC (Step 3.1). The Pharmacy portal automatically checks these VPs according to the verification policies (Step 3.2) and the prescription status from the blockchain to prevent prescription double-spending (Step 3.3). Then, it issues an invoice VC to the patient. The patient scans the QR code to receive the invoice (Step 3.4) and performs the payment through the SSI-MedRx smart contract (see Algorithm 1). The pharmacy receives the medications to the patient once it gets a notification that the correct amount is paid (Step 3.6).

4) Issuance of refund request VC by pharmacy: The pharmacy can issue a refund request VC immediately after dispensing the prescription and present it to insurance (Steps 4.1 and 4.2). The pharmacy does not need to keep a copy of the patient's prescriptions. The refund request VC includes the same information as the invoice VC and the prescription VP presented by the patient.

5) Verification of refund request VP and reimbursement by insurance: Upon receiving the refund request VP from the pharmacy, the insurance conducts checks to determine the validity of the refund request VP and the prescription VP according to the verification policies (Step 5.1). It also verifies whether the prescription has been dispensed and has not been refunded and confirms that the payment has been directed to the registered pharmacy address (Step 5.2). Since the SSI-MedRx smart contract also verifies these conditions (see Algorithm 2), the insurance company performs these checks before initiating the refund request in Step 5.3 to prevent any failure in the refund transaction.

4. Implementation

This section outlines the implementation specifics of the SSI-MedRx platform, addressing details ranging from configuration to the issuance and verification of VCs. It emphasizes components used to combat fraud and ensure interoperability.

We have used various tools and frameworks to implement the SSI-MedRx Proof of Concept (PoC). Specifically, Docker and Docker Compose [31] were used to containerize and orchestrate the deployment of the system's components. This setup facilitated the development and testing of the backend, frontend, and various portals, ensuring a consistent and scalable environment. We also used Walt.id's Wallet Kit [32] as the API and backend framework to provide the core infrastructure for managing SSI capabilities, including verifiable credentials and decentralized identifiers. The Wallet Kit serves as the backend business logic for the SSI-MedRx wallet and includes a reference implementation of the verifier and issuer portal backends. In addition, we used Nginx [33] as a reverse proxy that intermediates user calls to the wallet frontend, government portal, doctor portal, and pharmacy portal, ensuring efficient routing and load distribution across these services.

4.1. Issuers configuration and creation of credential schemas

Through Walt.id REST APIs [34], we configured the trusted issuers of VCs, which are supposed to be performed by the governance authority. We created DIDs for the government/insurance authority, healthcare authorities, doctors, and pharmacies. Then, we set their configuration files using the generated DIDs. Besides the DID, the configuration file includes credential types that issuers can issue, as shown in Fig. 4. In this example, the doctor is allowed to issue only prescriptions. After that, we created schemas for the following credentials: identity card, insurance card, healthcare professional ID, prescription, invoice, and refund request. Fig. 5 shows an example of prescription schemas that a doctor should use to issue the prescription. In real scenarios, governance authorities may onboard only government authorities globally and authorize them to onboard other issuers (i.e., healthcare authorities, doctors, and pharmacies) in their respective countries.


```
{
   "credentialTypes": ["Prescription"],
   "issuerApiUrl": "http://localhost:8080/issuer-api/defaultb",
   "issuerClientName": "Doctor Portal",
   "issuerDid": "did:key:z6MkknqukiVL7BWcB9ASUtkeL8CUe7QKw4b9hnnuwrnDAU3A",
   "issuerUiUrl": "http://localhost:8001",
   "wallets": {
      "waltid": {
         "description": "walt.id web wallet",
         "id": "waltid",
         "presentPath": "api/siop/initiatePresentation/",
         "receivePath": "api/siop/initiateIssuance/",
         "url": "http://localhost:3000"
      }
   }
}
```


Fig. 4. Doctor configuration JSON file example.


```
{
   "type": [
      "VerifiableCredential",
      "Prescription"
   ],
   "@context": [
      "https://www.w3.org/2018/credentials/v1"
   ],
   "issuer": "",
   "issuanceDate": "2023-08-25T00:00:00Z",
   "issued": "2023-08-25T00:00:00Z",
   "validFrom": "2023-08-25T00:00:00Z",
   "credentialSubject": {
      "doctorName": "Dr. Sarah Johnson",
      "doctorId": "DR12345",
      "patientName": "John Doe",
      "patientId": "PAT67890",
      "dateOfBirth": "1990-05-15",
      "gender": "MALE",
      "medications": [
         {
            "drugName": "Paracetamol",
            "quantity": "2",
            "frequency": "Once daily"
         }
      ],
      "refill": "2"
   }
}
```


Fig. 5. Prescription credential schemas.

4.2. Development of SSI-MedRx system

The governance authority is responsible for the development of the SSI-MedRx. It must provide open access to the source code to ensure

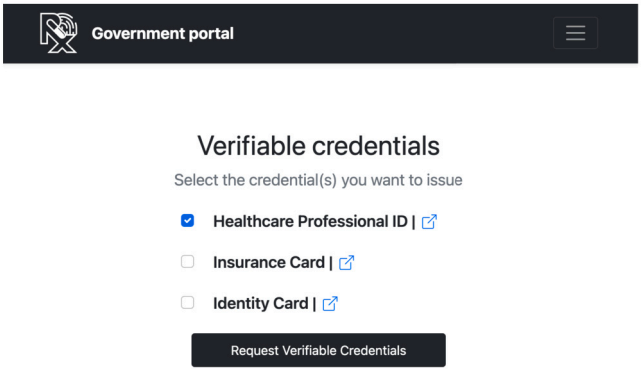

Fig. 6. Government portal.

transparency, allowing regulatory bodies from various nations to review it before utilization. SSI-MedRx system offers a wallet and web portals for different stakeholders and a web/mobile wallet for patients. The SSI-MedRx web portals were developed using Vue.js and Nuxt.js [35].

The SSI-MedRx and MedRx token smart contracts were written in the Solidity programming language. When it comes to the SSI-MedRx mobile/web wallet, we used Walt.id's web wallet [36] to develop our healthcare wallet. In addition to managing patients' personal and health data, this wallet aims to protect patients from opioid addiction, which is enforced through code. Regarding the payment, we utilized the Metamask crypto-wallet [37]. To avoid redundant code, we created a single portal for both government/insurance authorities and healthcare authorities, which we refer to as the "government portal" for short (see Fig. 6). We also established two separate portals for doctors and pharmacies respectively. Additionally, we deployed the MedRx Token and SSI-MedRx smart contracts on the Polygon test network. Because SSI-MedRx relies on Walt.id APIs to access different SSI features and these APIs currently do not support DID: polygon, we used the DID: Key method for both issuers and patients.

Algorithm 1: Pay medications function.

```
Data: string memory _prescriptionId, uint256 TotalAmount, address
      _pharmacyAddress
Result: Payment transaction and prescription status
if prescriptions[_prescriptionId].status == PrescriptionStatus.NotSpent
 then
    if msg.value == TotalAmount then
        MedRxToken token =
          MedRxToken(MedRxTokenContractAddress);
        token.transfer(payable(_pharmacyAddress), TotalAmount);
        listOfPaidRx.push(_prescriptionId);
        prescriptions[_prescriptionId].amount = TotalAmount;
        prescriptions[_prescriptionId].pharmacyAddress =
          _pharmacyAddress;
        prescriptions[_prescriptionId].status =
          PrescriptionStatus.Spent;
    end
    else
        Revert("The received amount is not equal to the total amount
          in the invoice");
    end
end
else
    Revert("Prescription already paid or spent");
end
```

Algorithm 2: Refund pharmacy function.

```
Data: string memory _prescriptionId, address
      RegistredPharmacyAddress
Result: Refund trusted pharmacy
if prescriptions[_prescriptionId].status == PrescriptionStatus.Spent then
    if prescriptions[_prescriptionId].pharmacyAddress ==
     RegistredPharmacyAddress then
        if prescriptions[_prescriptionId].refunded == false then
            MedRxToken token =
              MedRxToken(MedRxTokenContractAddress);
            token.transfer(payable(RegistredPharmacyAddress),
              msg.value);
            listOfRefundedRx.push(_prescriptionId);
            prescriptions[_prescriptionId].refunded = true;
        end
        else
            Revert("The pharmacy has already been refunded");
        end
    end
    else
        Revert("This pharmacy address is not registered, cannot be
          refunded");
    end
end
else
    Revert("This Prescription has not been spent, cannot be refunded");
end
```

The primary objective of the SSI-MedRx smart contract, which includes two main functions named Pay Medications and Refund Pharmacy, is to enforce anti-insurance fraud policies through code. The first function, as illustrated in Algorithm 1, allows the patient to pay the pharmacies, while the second enables insurance to reimburse the pharmacies (see Algorithm 2). The insurance can ensure that 1) the prescription has been paid or spent through this contract, 2) payment was made to a registered, trusted pharmacy address, 3) prescription has not been refunded. However, the smart contract provides no prescription details besides its identifier. The confidential information is transferred to the insurance off-chain through a refund request VC issued by the pharmacy. These verifiable credentials include information related to the medication price, the amount that should be refunded, and the prescription VP that the patient shared to get the medications. In this way, the insurance can read confidential data and verify whether the prescription is legitimate and is shared with the patient's consent.

Fig. 7 shows an example of a prescription verifiable presentation signed by a patient (did:key:z6Mkqz gFp7ccbiH6e n6cZrnbKdfY2V4kGWftQKux2G92KWrD) which includes a prescription VC signed by a doctor identified by the following DID: "did:key:z6MknqukiVL7BWcB9ASUtkeL8CUe7QK w4b9hnnuwrnDAU3A". The insurance can confirm the patient's consent by verifying that the VP is signed with the patient's private key related to the same DID written in the credentialSubject.

Hence, the SSI-MedRx smart contract, combined with the prescription verifiable presentation included in the refund request VC, enables SSI-MedRx to prevent phantom billing effectively.

4.3. Credentials issuance by the root of trust

In our use case, the government/insurance entity acts as the root of trust for issuing identity and insurance card VCs to citizens. At the same time, the healthcare authority serves as the root of trust for issuing healthcare professionals' card ID VCs. As mentioned earlier, we developed a single portal for both of these entities, as depicted in Fig. 6, because from a technical perspective, it utilizes the same code. Before issuing VCs, government employees adhere to the Know Your Customer (KYC) process to validate citizens' or healthcare providers' identities and

```
{
  "type": [
    "VerifiablePresentation"
  ],
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/security/suites/jws-2020/v1"
  ],
  "id": "urn:uuid:731084d2-8479-4a54-9eb2-08c71d81ba4c",
  "proof": { // Proof of the verifiable presentation
    "type": "JsonWebSignature2020",
    "creator": "did:key:z6MkqzgFp7ccbiH6en6cZrnbKdfY2V4kGWftQKux2G92KWrD",
    "created": "2023-10-31T10:59:06Z",
    "proofPurpose": "authentication",
    "verificationMethod": "did:key
       :z6MkqzgFp7ccbiH6en6cZrnbKdfY2V4kGWftQKux2G92KWrD#z6MkqzgFp7ccbiH6en6c
       ZrnbKdfY2V4kGWftQKux2G92KWrD",
    "jws": "eyJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdLCJhbGciOiJFZERTQSJ9..alqoY
       --s2YwnGuJuBYHchtKr4Ybbm1NoKzQOQTKfx67Q8Bh_mY5MqRNBMQNUIK3wXm2xnRMm_EW
       1Qcndw-Q4CQ",
    "nonce": "wmu67ilFSF-EorPljzFFPw"
  },
  "holder": "did:key:z6MkqzgFp7ccbiH6en6cZrnbKdfY2V4kGWftQKux2G92KWrD",
  "verifiableCredential": [
    {
      "type": [
        "VerifiableCredential",
        "Prescription"
      ],
      "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://w3id.org/security/suites/jws-2020/v1"
      ],
      "id": "urn:uuid:a75737e5-119d-420b-8982-111c06203986",
      "issuer": "did:key:z6MkknqukiVL7BWcB9ASUtkeL8CUe7QKw4b9hnnuwrnDAU3A",
      "issuanceDate": "2023-10-31T10:56:48Z",
      "issued": "2023-10-31T10:56:48Z",
      "validFrom": "2023-10-31T10:56:48Z",
      "proof": { // proof of this verifiable credential
        "type": "JsonWebSignature2020",
        "creator": "did:key
           :z6MkknqukiVL7BWcB9ASUtkeL8CUe7QKw4b9hnnuwrnDAU3A",
        "created": "2023-10-31T10:56:48Z",
        "verificationMethod": "did:key
           :z6MkknqukiVL7BWcB9ASUtkeL8CUe7QKw4b9hnnuwrnDAU3A#z6MkknqukiVL7B
           WcB9ASUtkeL8CUe7QKw4b9hnnuwrnDAU3A",
        "jws": "eyJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdLCJhbGciOiJFZERTQSJ9
           ..dkMjHBjg1cKktncI
           -DteKecDONnNxnKWHaRo6Ixl7H1sV6GouIfWJi9our3IZFoEA2yuwVDFe6T
           -4J23J9PhCQ"
      },
      "credentialSubject": {
        "id": "did:key:z6MkqzgFp7ccbiH6en6cZrnbKdfY2V4kGWftQKux2G92KWrD",
        "doctorName": "Dr. John Smith",
        "doctorId": "DR34562456",
        "patientName": "Meriem Guerar",
        "patientId": "09040080833G",
        "dateOfBirth": "1990-07-01",
        "gender": "FEMALE",
        "medications": [
          {
            "drugName": "Fexofenadine",
            "quantity": "2",
            "frequency": "Once daily"
          }
        ],
        "refill": "2"
      }
    }
  ]
}
```


Fig. 7. Prescription verifiable presentation in JSON-LD format.

required documents, including passports, birth certificates, proof of residency, and medical licenses. Citizens and healthcare providers need to scan the QR code (as shown in Fig. 8) using their SSI-MedRx wallets and provide consent to receive the VCs in their purses.

4.4. Healthcare professionals authentication

Fig. 9 shows the doctor portal login page. To log in, healthcare professionals must scan a QR code to present their healthcare professional ID VCs issued by the government. They will be authorized to access the platform if the verification is successful. SSI-MedRx utilizes the following Walt.id built-in policies, namely SignaturePolicy, JsonSchemaPolicy, ChallengePolicy and PresentationDefiniti onPolicy. Walt.id also offers CredentialStatusPolicy to verify whether the status is still valid (i.e., not expired or revoked). Additionally, we created

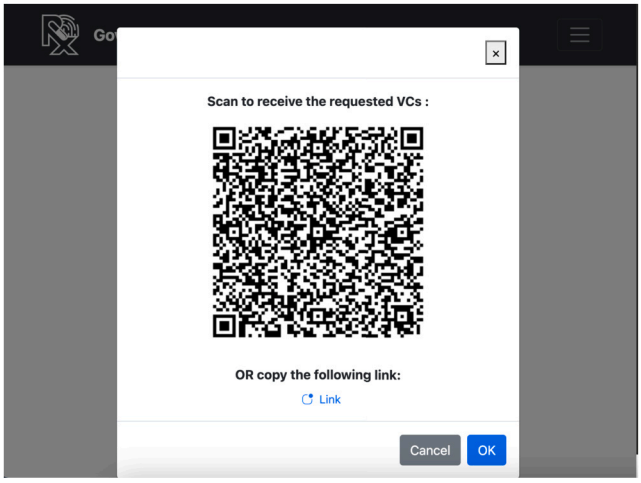

Fig. 8. QR code or deep link that can be used to initiate credentials issuance.

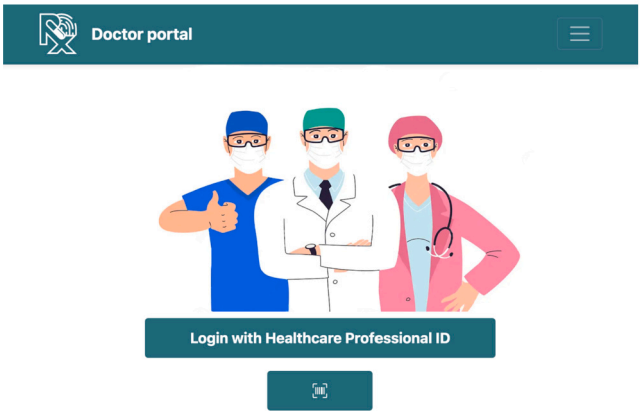

Fig. 9. Doctors portal login page.

a custom policy to verify the role the healthcare professionals, i.e., RolePolicy.

4.5. Verifiable credentials issuance and verification

We have opted for OpenID (OID4VC) to manage credential issuance and presentation, which includes three protocols aimed at enabling self-controlled authentication (SIOPv2), credential issuance (OID4VCI), and credential presentation (OID4VP) [29].

Once the doctors log in to their portal, they can start issuing prescription VCs. But before that, they have to verify the patient's identity. SSI-MedRx doctor portal displays a QR that encodes the authorization request URI along with essential request parameters, such as scope, presentation_definition, response_type, redirect_uri, state, nonce, client_id, and response_mode. We set the response_mode to post and response_type to vp_token. The patient must scan the QR code using their SSI-MedRx wallet and then accept the sharing of his/her ID VC. After getting the user consent, the wallet prepares the verifiable presentation of the Identity Card VC and posts the authorization response to the redirect_uri specified in the authorization request via the HTTP POST method. The SSI-MedRx doctor portal verifies the authorization response according to the verification policies. If the verification is successful, the page will be refreshed and redirected to the page shown in Fig. 10. The prescription form will be filled out with the doctor's and patient's information. The doctor only has to fill in the treatment details. Once

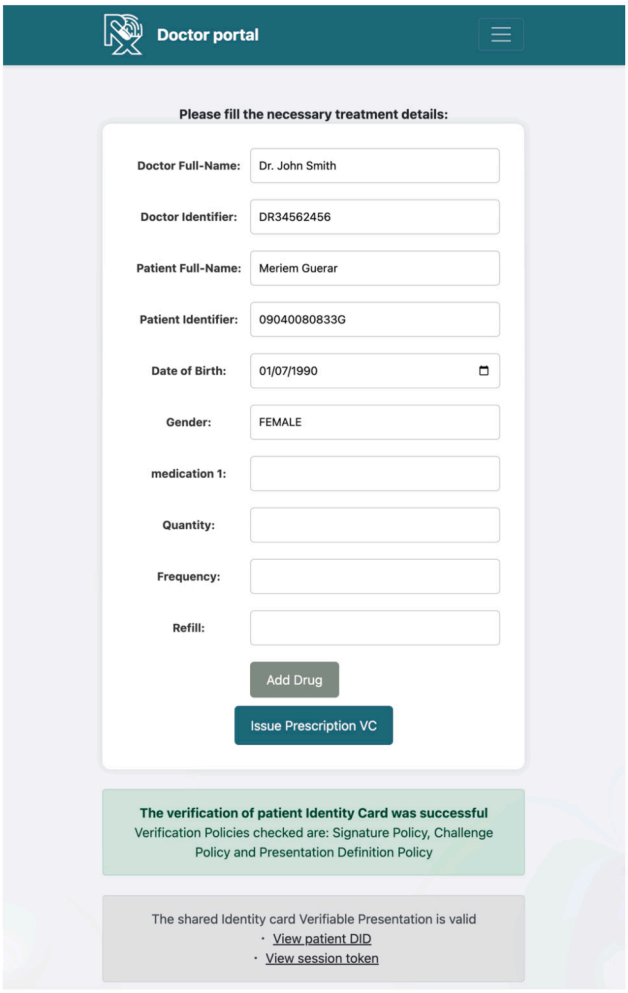

Fig. 10. Prescription form.

the patient scans the QR code and accepts receiving the VC, the prescription will be added to their wallet, as shown in Fig. 11. To get medications, patients must present their prescription, identity, and insurance cards by scanning a QR code, as shown in Fig. 12. An invoice form will be displayed once the verification of VPs using the policies has been completed successfully. The pharmacy can issue an invoice VC for the patient and a refund request VC for insurance through the platform. For the refund request, VC includes the same information in the invoice and a prescription VP presented by the patient. Once patients receive the invoice, they can pay the pharmacy and get the medications. Finally, the insurance verifies the VC refund request and reimburses the pharmacy.

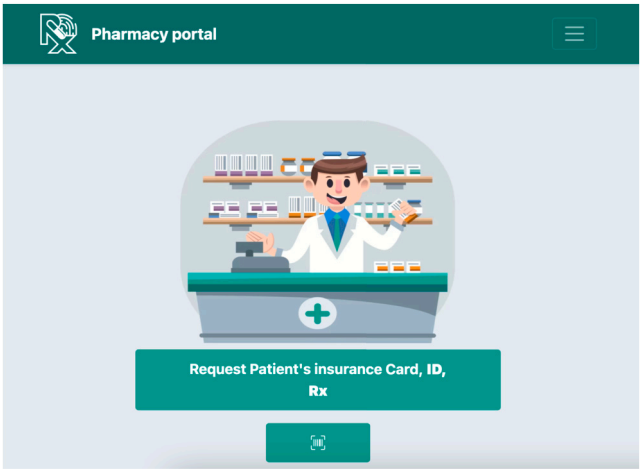

Fig. 12. Patient's credential verification page in the pharmacy portal.

5. Discussion

This section discusses how SSI-MedRx deals with the frauds and privacy concerns described in section 2.

5.1. Countermeasures against medical identity theft

Medical identity theft is a significant concern in the healthcare industry, and it can occur through various means, including insider threats from healthcare providers and external threats from attackers who gain unauthorized access to centralized databases. In the SSI-MedRx system,

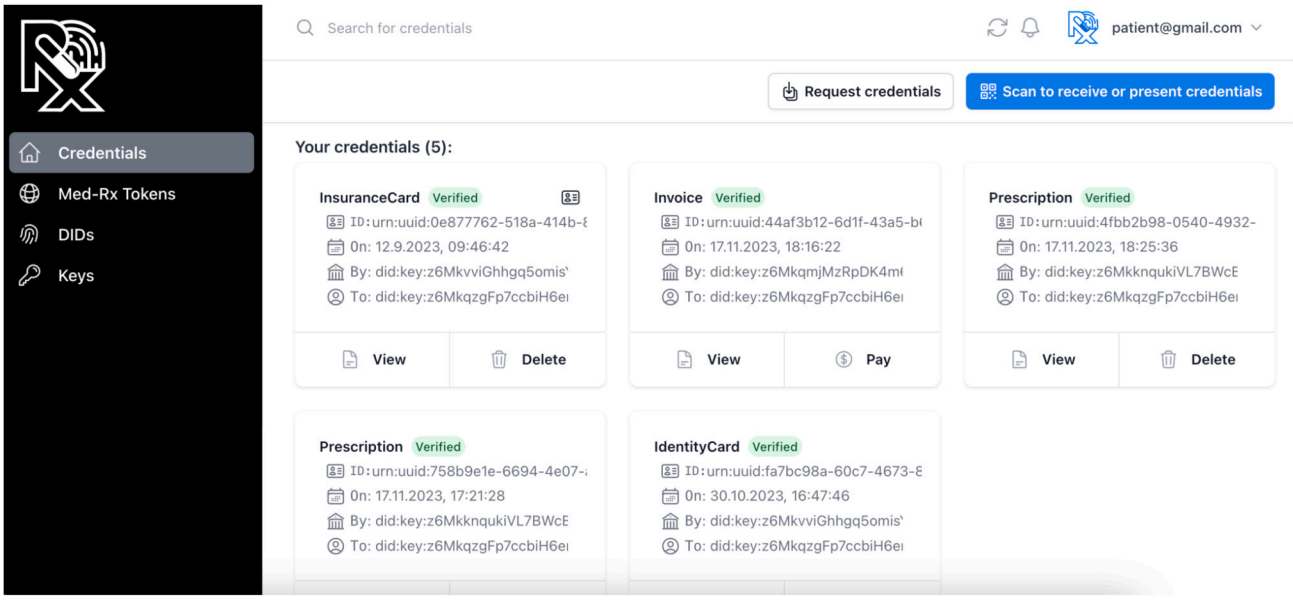

Fig. 11. List of verifiable credentials in the patient's wallet.

patient personal and health-related information is securely maintained within an isolated and safeguarded execution space, such as the Trusted Execution Environment (TEE) [27,38,39] inside patient devices, eliminating the need for a centralized database. Thus, the lack of a central database for attackers to target significantly reduces the risk of data breaches. Attackers may try to compromise patient devices. However, bypassing the authentication mechanisms of both the device and the wallet is highly challenging. The returns are limited even if they successfully access the private key stored in secure hardware. The attacker would only gain access to the information of a single patient, unlike in centralized systems where an entire database could be compromised.

On the other hand, healthcare professionals can also commit medical identity theft. Since patient data are not stored in a centralized database by SSI-MedRx, patients must share the necessary information whenever they need a service. Sharing this information with healthcare providers involves authentication of their wallets and the patient's explicit consent. Patients grant consent by clicking "Accept" to share the VC when they receive a request in their SSI-MedRx wallet. In the background, the SSI-MedRx wallet signs the verifiable credentials using their private keys. Therefore, the act of insiders stealing patient information for future misuse [14] is not sufficient to impersonate patients; the perpetrators would also need to possess the patient's private keys. This is one of the advantages of leveraging SSI—you need to know the information and have the private keys to prove ownership of this information, which adds a layer of security. Additionally, unethical healthcare providers may attempt to replay the verifiable presentation received by the patient to impersonate them. SSI-MedRx prevents VP replay attacks by incorporating a challenge policy and ensuring that the holder of the VP is the same as the subject DID in the verifiable credential.

5.2. Countermeasures against phantom billing

SSI-MedRx ensures that pharmacies cannot fraudulently claim reimbursement from insurance for items that are not dispensed, preventing them from benefiting from such fraudulent claims.

This is because SSI-MedRx forces the pharmacies to share a refund request VC, which, in addition to the invoice, should include the prescription VP provided by the patient. This allows the insurance company to check the authenticity of the prescription by verifying the doctor's signature and confirming whether the data are shared with the patient's consent by verifying that the patient signed the prescription VP. Any modification leads to an invalid signature, and impersonating these parties, as mentioned earlier, necessitates their private keys. In addition, SSI-MedRx leverages blockchain to track the prescription status and payment sent to pharmacies. The status is automatically updated to "spent" by the SSI-MedRx smart contract upon the patient's payment and is immutable. Thus, the insurance could check 1) check whether the respective pharmacy has dispensed the prescription by reading its status from the blockchain, 2) confirm the authenticity of a prescription, and 3) ensure that patient data are shared with explicit consent. Therefore, our system provides robust protection against fraudulent billing.

5.3. Countermeasures against kickbacks

SSI-MedRx addresses kickback fraud by allowing doctors to prescribe drugs using their chemical names rather than brand names. When a patient chooses a pharmacy for payment, SSI-MedRx presents options available at that specific pharmacy. Patients can then decide whether to purchase the generic or brand-name drug based on factors such as price, the drug's reputation, or personal preferences. This approach prevents doctors from prescribing medications solely for financial incentives and ensures that pharmacies cannot favor specific drug brands over others.

5.4. Countermeasures against opioid overprescribing

In the SSI-MedRx ecosystem, the governance authority pragmatically enforces an anti-addiction rule. The patient's SSI-MedRx wallet will only accept the prescription VC from the doctor if the prescribed drug, in combination with the patient's ongoing treatments, does not exceed the permissible dosage of substances that could lead to addiction, such as opioids. This approach eliminates the need for doctors to manually check patient's history through PDMP databases, which may not always be current. Whether doctors prescribe opioids with good intentions or to receiving kickbacks, SSI-MedRx protects patients from receiving prescriptions that could lead to addiction, regardless of the geographic location of the doctor they visit.

5.5. Privacy concern

Using SSI-MedRx, the patient's personal and health data are stored in secure hardware in their devices and are shared only with their consent. The sensitive information in VCs and VPs is securely transferred off-chain between the different parties through a mutually authenticated and encrypted data channel between the communicating parties. The most common data exchange protocols are DIDComm [40] and OID4VC [29]. SSI-MedRx uses OID4VC. It is worth mentioning that no personal or sensitive data are stored on a centralized database or blockchain. The data stored on the blockchain include the credential templates, trusted issuer DIDs, and DID documents, which include a public key used for the issuer's signature verification. In addition, the blockchain stores prescription status and the history of payment transactions used to prevent double-spending and insurance fraud. The other confidential prescription details, such as the patient's personal information, drugs, quantities, and dosage, are stored on the patient's device and are exchanged off-chain.

5.6. Data breaches

SSI-MedRx adopts a decentralized and user-centric approach, eliminating a central database for attackers to target, thus significantly reducing the risk of data breaches. Patients' healthcare data and keys are securely stored in the SSI-MedRx wallet on their mobile devices. The wallet resides within a TEE, ensuring isolation from applications within the Rich Execution Environment (REE) while maintaining the integrity and confidentiality of the processed information. Moreover, encryption keys are securely stored within dedicated hardware components, such as secure elements. In this way, compared with centralized databases, SSI-MedRx decreases the value of data stored in each device and increases the cost of accessing it, reducing the attacker's incentive to target individual devices for data breaches.

6. Related work and comparison

In recent years, considerable research has investigated the integration of blockchain technology in the healthcare sector [41–51], with relatively few studies exploring SSI. In this section, we select the works most relevant to our proposed system.

Abid et al. [7] introduced NovidChain, a decentralized platform based on the SSI model for managing COVID-19 tests or vaccine certificates. Through their platform, patients receive their certificates in the form of verifiable credentials. These credentials are encrypted on IPFS,

while their corresponding hashes are recorded on-chain to ensure data integrity. The patient can then share the VCs with authorized verifiers through their uPort wallets to gain access to various public spaces. However, NovidChain employs a private permissioned blockchain to record the DIDs of trusted issuers. This approach, while ensuring privacy, restricts unregistered verifiers from validating certificates. This limitation somewhat diminishes the advantages of using vaccine certificate VCs, which are intended to be borderless.

Hasan et al. [52] proposed a blockchain-based solution for COVID-19 digital medical passports and immunity certificates. Medical test results, residency information, and identity documents are encrypted on IPFS, with only their hashes recorded on the blockchain to reduce costs and ensure data integrity. Since patients must provide access to these documents to various authorities, the authors implemented a proxy re-encryption scheme. This approach eliminates the need for patients to re-encrypt documents for each new authorization or recipient. Instead, they can delegate access using re-encryption keys. Furthermore, the authors integrated a decentralized key management system to retrieve the recipient's public key, which is necessary to generate the re-encryption key. While referencing blockchain-based identity management systems such as Sovrin, uPort, and ShoCard in their work, the authors did not delve into the specifics of their implementations. Besides, the patient's smart contract deployed in the public Ethereum blockchain includes personal information such as gender, name, date of birth, and travel history, which raises privacy concerns.

Harrell et al. [53] introduced MediLinker, an SSI-based solution that facilitates healthcare data exchange through verifiable credentials among clinics. However, in their proposed system, clinic receptionists are responsible for verifying the patient's physical identity card and manually entering this information to issue a health ID VC, which can be used later to identify patients without physical IDs in other clinics. Furthermore, MediLinker opts for a cloud-based wallet, which offers advantages such as lightweight implementation and cross-platform accessibility. However, this wallet type often necessitates reliance on third-party services, requires internet connectivity, and may not provide the same level of control and ownership that aligns with the core principles of self-sovereign identity. In addition, the authors used Amazon Web Services (AWSs), a centralized cloud service provider, to host Hyperledger Indy servers and Hyperledger Aries agents.

In Ref. [54], the authors introduced an SSI-based Health Passport integrated with a cloud-based Personal Health Record (PHR) system named MediTrans. Their solution enables patients to access their medical records from the hospital's Electronic Medical Record (EMR) system and store them in the MediTrans cloud, which can be converted into VCs. While their approach facilitates the sharing of medical history among different hospitals, it is important to note that the reliance on the MediTrans cloud creates a potential single point of failure, making the system susceptible to data breaches.

Heisenberg project [55] introduced a decentralized application built on top of a private permissioned blockchain to monitor prescriptions. In this system, doctors issue prescriptions as ERC-721 tokens to patients, which are subsequently transferred to the pharmacy address by the patient to receive the prescribed medications. While this approach effectively prevents prescription double spending, it has certain drawbacks. Doctors must cover the deployment cost of prescription smart contracts for each medication, and patients are responsible for the expense associated with the transfer. Furthermore, details about the onboarding process for doctors into the system have not been provided. On the other hand, the non-fungible tokens carry metadata on the blockchain, including details such as the doctor's ID, the patient's public key, medication name, quantity, dosage, and expiry date, which raises privacy concerns. All the blockchain network members are able to read the patient's prescription details.

Similarly, Cilli et al. [9] introduced safe prescription, which tokenizes patient prescriptions using the ERC-721 standard and stores the data on a permissioned Ethereum-based blockchain. In their system, the National Health Service (NHS) is responsible for contract deployment costs and onboarding doctors and pharmacies. Authorized doctors issue prescription NFTs, which patients must transfer to pharmacies to obtain their medications. Subsequently, the pharmacies transfer these NFTs and invoices to the NHS for reimbursement. Although the NHS can track the prescription's transfer to the pharmacy with the patient's consent, this is not enough to prevent phantom billing because it does not offer proof that the prescription was dispensed.

Schlatt et al. [8] proposed an e-prescription management system based on blockchain technology and the SSI model to harmonize sensitive data exchange and prevent double-spending. It's worth emphasizing that double spending is typically not a concern in traditional centralized systems. However, when applying the SSI model for prescription exchange, patients hold verifiable credentials in their wallets, allowing them to be presented whenever they want. Thus, to prevent double-spending, the authors suggested recording the times the prescription can be spent on the blockchain. The doctor must create a smart contract that includes a function that has to be called by the pharmacy to decrease this count each time the prescription is dispensed. Since the doctor cannot know the pharmacy address during the contract creation, they must generate a key pair (skpresc, pkpresc) for each prescription they issue. The private key is then included in the E-prescription verifiable credential, which is shared with the patient. Therefore, the patient should only present the e-prescription VC to a trusted pharmacy. The limitation of this approach is that anyone who possesses the private key, including the doctor, can invalidate the token preventing the patient from receiving the prescribed medication, and there is no way to know who is responsible and hold them accountable for their actions. Furthermore, the authors utilized Hyperledger Indy to verify identity and manage verifiable credentials and Quorum, a private blockchain, to track the prescription status counter. Apart from the expenses related to deploying the smart contract and updating the state variable, there's an issue when a patient seeks to fill the prescription in a non-member country. In such cases, the pharmacy can verify the authenticity of the VC but cannot determine whether the prescription has already been spent.

Eisenstadt et al. [56] developed a mobile application prototype for managing COVID-19 antibody tests or vaccine certifications. Unlike centralized systems, patients' data are stored in Solid Pods [56] hosted on their mobile devices. The onboarding of issuers involves a two-factor authentication process. Initially, they must complete a form with correct information and provide a valid official email address associated with the company's registered domain name. The application generates DIDs for the issuers when they complete the verification by tapping on the link sent to their email address. On the other hand, patients are required to upload a photo of an identification document within the application, such as a driving license or passport. The application stores the document's hash on the blockchain and generates a DID for the patient, stored on their solid pods. Every time the application runs an operation, it requests the user's permission to read the data stored on their Solid Pods. Once the healthcare providers verify the patient's identity through the application, they conduct the antibody test and create the vaccination certificate as a VC. The hash of this certificate is also stored on the blockchain. However, the authors used a consortium-permissioned blockchain, restricting non-members from verifying the VC certificate.

Fig. 13 summarizes the comparison of SSI-MedRx with the existing systems in the literature according to the requirements defined in section 3.1.

References	Blockchain Type	Blockchain purpose	SSI purpose & components	Security features					Privacy		Countermeasures against healthcare frauds			Interoperability	Borderless
				SSI-based authentication	Decentralized storage	Secure data exchange	Full control & ownership	Public verifiability & authenticity	Data Confidentiality	Auditable consent	Phantom billing	Kickbacks	Opioid overprescribing		
NovidChain [7]	Private permissioned blockchain	Trusted issuers registry (DID, name, medical ID and account address). Trusted verifiers registry. Credential schema. Hash of patient personal data and Covid-19 test results.	VCs for COVID-19 test/vaccine certificates	x	✓	✓	x	✓	✓	✓	x	x	x	✓	x
Hasan et al. [52]	Public permissionless blockchain	Record gender, name, date of birth, visited countries details and Covid-19 test dates. Hash of Medical test results, residency information, and identity documents.	DKMS for managing user's DIDs and private keys and DID auth to prove control over a DID.	-	✓	✓	x	✓	x	x	x	x	x	x	✓
MediLinker [53]	Public permissioned blockchain	Trusted issuers registry Credentials schemas	VCs for health ID, medications, insurance, credit card, research consent and Medical Power of Attorney (MPOA)	x	x	✓	x	✓	✓	✓	x	x	x	✓	x
Health Passport [54]	Public permissioned blockchain	Trusted issuers registry Credentials definition Credentials schema Revocation registry	VCs for health records	x	x	✓	x	✓	✓	✓	x	x	x	✓	✓
Heisenberg project [55]	Private permissioned blockchain	List of trusted doctors IDs. Prescriptions as NFT Smart Contracts (the doctor ID, the patient's public key, the medication name, quantity, dosage, and expiry Date).	-	-	✓	✓	x	x	x	✓	x	x	x	x	x
Safe Prescription [9]	Private permissioned blockchain	Prescriptions as NFT Smart Contracts	-	-	✓	✓	x	x	x	✓	x	x	x	x	x
Schlatt et al. [8]	Public & private permissioned blockchain	Doctor address and counter. Trusted issuers registry. Credentials definition. Credentials schema. Revocation registry.	VCs for Insurance card and prescriptions.	-	x	✓	x	✓	✓	✓	x	x	x	✓	x
Eisenstadt et al. [56]	Consortium permissioned blockchain	Hash of holder identification documents and COVID-19 test results	VC for DID ownership VCs for COVID-19 test/vaccine certificates	x	✓	-	✓	x	✓	✓	x	x	x	x	x
SSI-MedRx	Public permissioned/ permissionless blockchain	Payment transactions, refund status and prescription status. Trusted issuers registry. Credentials schema.	VCs for healthcare professionals ID, insurance card, identity card, prescriptions, health records, invoices and refund request.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Fig. 13. Related work and comparison.

7. Conclusion

In recent years, we have witnessed several high-profile healthcare data breaches that have exposed sensitive patient records to unauthorized access. Besides data breaches that threaten patient privacy and security, the current systems lack the necessary security measures to prevent healthcare fraud, which leads to financial losses and poses significant risks to patient safety and healthcare services. Addressing these fraudulent activities is crucial for protecting insurance, safeguarding patient well-being, and ensuring the effectiveness of healthcare services. This paper provides guidelines for designing a borderless, fraud-resilient, and privacy-preserving healthcare system. Additionally, we introduced a novel healthcare system based on blockchain and SSI to combat complex healthcare frauds, such as medical identity theft, phantom billing, kickbacks, and opioid overprescribing. Our system enables cross-border interoperability and accessibility while safeguarding user privacy and granting patients complete control over their data. Furthermore, we emphasize the advantages of SSI-MedRx over the existing healthcare systems in the literature. In future work, we plan to evaluate various public permissioned and permissionless blockchain networks (e.g., Ethereum, Hyperledger Besu, and Hyperledger Indy) in terms of scalability, cost, and performance for supporting decentralized identity-related operations, tracking payment and status verification. Additionally, we intend to explore the potential of AI and IoT devices to further enhance our system and user experience. For instance, AI can analyze the patient's genetic data to predict potential health risks or susceptibilities to specific diseases based on genetic markers. AI can also be leveraged to assess the risk of adverse drug reactions or inefficacy based on the genetic profile.

CRediT authorship contribution statement

Meriem Guerar: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Project administration, Methodology, Investigation, Conceptualization. **Mauro Migliardi:** Writing – review & editing, Validation, Supervision, Investigation. **Enrico Russo:** Writing – review & editing, Visualization, Methodology. **Djamel Khadraoui:** Writing – review & editing, Validation. **Alessio Merlo:** Writing – review & editing, Validation, Supervision, Investigation, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was partially supported by project SERICS - "Security and Rights in CyberSpace" (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

[1] J. Villegas-Ortega, L. Bellido-Boza, D. Mauricio, Fourteen years of manifestations and factors of health insurance fraud, 2006–2020: a scoping review, Health & Justice 9 (1) (2021) 1–23, https://doi.org/10.1186/s40352-021-00149-3.

[2] N.F. Stowell, C. Pacini, N. Wadlinger, et al., Investigating healthcare fraud: its scope, applicable laws, and regulations, William & Mary Bus. Law Rev. 11 (2) (2020) 479.

[3] B.M. Gray, J.L. Vandergrift, W. Weng, et al., Clinical knowledge and trends in physicians' prescribing of opioids for new onset back pain, 2009-2017, JAMA Netw. Open 4 (7) (2021) e2115328, https://doi.org/10.1001/jamanetworkopen.2021.15328.

[4] M. Guerar, A. Merlo, M. Migliardi, et al., A fraud-resilient blockchain-based solution for invoice financing, IEEE Trans. Eng. Manag. 67 (4) (2020) 1086–1098, https://doi.org/10.1109/TEM.2020.2971865.

[5] M. Guerar, L. Verderame, A. Merlo, et al., Blockchain-based risk mitigation for invoice financing, in: Proceedings of the 23rd International Database Applications & Engineering Symposium, Ser. IDEAS '19, ACM, 2019, https://doi.org/10.1145/3331076.3331093.

[6] M. Guerar, M. Migliardi, Truthseekers chain: leveraging invisible cappcha, SSI and blockchain to combat disinformation on social media, in: O. Gervasi, B. Murgante, S. Misra, et al. (Eds.), Computational Science and Its Applications – ICCSA 2022 Workshops, Springer, Cham, 2022, pp. 419–431, https://doi.org/10.1007/978-3-031-10542-5_29.

[7] A. Abid, S. Cheikhrouhou, S. Kallel, et al., NovidChain: blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates, Softw. Pract. Exp. 52 (4) (2022) 841–867, https://doi.org/10.1002/spe.2983.

[8] V. Schlatt, J. Sedlmeir, J. Traue, et al., Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: the case of e-prescription management, Distrib. Ledger Technol. 2 (1) (2023) 841–867, https://doi.org/10.1145/3571509.

[9] C. Cilli, E.G. Magnanini, M. Silipigni, et al., "Safe prescription": a decentralized blockchain protocol to manage medical prescriptions, in: Proceedings of the Italian Conference on Cybersecurity, CEUR-WS, 2022, https://ceur-ws.org/Vol-3260/paper3.pdf.

[10] B. Aldughayfiq, S. Sampalli, Digital health in physicians' and pharmacists' office: a comparative study of e-Prescription systems' architecture and digital security in

eight countries, Omics. J. Integr. Biol. 25 (2) (2021) 102–122, https://doi.org/10.1089/omi.2020.0085.
[11] IDX, Medical identity theft in the new age of virtual healthcare, https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare, 2021. (Accessed 8 November 2023).
[12] K. Permanente, Fifth annual study on medical identity theft, https://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf, 2015. (Accessed 8 November 2023).
[13] J. Lu, K. Lin, R. Chen, et al., Health insurance fraud detection by using an attributed heterogeneous information network with a hierarchical attention mechanism, BMC Med. Inform. Decis. Mak. 23 (1) (2023) 62, https://doi.org/10.1186/s12911-023-02152-0.
[14] U.S. Department of Justice, National health care fraud takedown results in charges against 301 individuals for approximately $900 million in false billings, https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-301-individuals-approximately-900, 2016. (Accessed 8 November 2023).
[15] H. Fresques, Doctors prescribe more of a drug if they receive money from a pharma company tied to it, https://www.propublica.org/article/doctors-prescribe-more-of-a-drug-if-they-receive-money-from-a/-pharma-company-tied-to-it, 2019. (Accessed 8 November 2023).
[16] U.S. Department of Justice, Opioid manufacturer purdue pharma pleads guilty to fraud and kickback conspiracies, https://www.justice.gov/opa/pr/opioid-manufacturer-purdue-pharma-pleads-guilty-fraud-and-kickback-conspiracies, 2020. (Accessed 8 November 2023).
[17] B.W. Gac, H. Yakubi, D.E. Apollonio, Issues arising from the study design, conduct, and promotion of clinical trials funded by opioid manufacturers: a review of internal pharmaceutical industry documents, Evidence & Policy 19 (4) (2023) 536–553, https://doi.org/10.1332/174426421X16856230946027.
[18] P. Zhang, B. Stodghill, C. Pitt, et al., OpTrak: tracking opioid prescriptions via distributed ledger technology, Int. J. Inf. Syst. Soc. Change 10 (2) (2019) 45–61, https://doi.org/10.4018/IJISSC.2019040104.
[19] F. Alogaili, N. Abdul Ghani, N. Ahmad Kharman Shah, Prescription drug monitoring programs in the US: a systematic literature review on its strength and weakness, J. Inf. Public Health 13 (10) (2020) 1456–1461, https://doi.org/10.1016/j.jiph.2020.06.035.
[20] PWC, Conti cyber attack on the HSE, Independent Post Incident Review, https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf, 2021. (Accessed 8 November 2023).
[21] E. Kost, 14 biggest healthcare data breaches, https://www.upguard.com/blog/biggest-data-breaches-in-healthcare, 2022. (Accessed 8 November 2023).
[22] V. Chiruvella, A.K. Guddati, et al., Ethical issues in patient data ownership, Interact. J. Med. Res. 10 (2) (2021) e22269, https://doi.org/10.2196/22269.
[23] M. Guerar, L. Verderame, M. Migliardi, et al., 2GesturePIN: securing PIN-based authentication on smartwatches, in: Proceedings of the 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), IEEE, 2019, pp. 327–333, https://doi.org/10.1109/WETICE.2019.00074.
[24] M. Guerar, M. Benmohammed, V. Alimi, Color wheel pin: usable and resilient ATM authentication, J. High Speed Netw. 22 (3) (2016) 231–240, https://doi.org/10.3233/JHS-160545.
[25] M. Guerar, A. Merlo, M. Migliardi, Clickpattern: a pattern lock system resilient to smudge and side-channel attacks, J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl. 8 (2) (2017) 64–78, https://doi.org/10.22667/JOWUA.2017.06.31.064.
[26] M. Guerar, M. Migliardi, F. Palmieri, et al., Securing pin-based authentication in smartwatches with just two gestures, Concurr. Comput. Pract. Exp. 32 (18) (2020) e5549, https://doi.org/10.1002/cpe.5549.
[27] M. Guerar, M. Migliardi, A. Merlo, et al., Using screen brightness to improve security in mobile social network access, IEEE Trans. Dependable Secure Comput. 15 (4) (2018) 621–632, https://doi.org/10.1109/TDSC.2016.2601603.
[28] M. Guerar, L. Verderame, A. Merlo, et al., CirclePIN: a novel authentication mechanism for smartwatches to prevent unauthorized access to IoT devices, ACM Trans. Cyber-Phys. Syst. 4 (3) (2020) 1–19, https://doi.org/10.1145/3365995.
[29] K. Yasuda, T. Lodderstedt, D. Chadwick, et al., OpenID for verifiable credentials, White Paper, openID. https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf, 2022. (Accessed 8 November 2023).
[30] J. Bruthans, The state of national electronic prescription systems in the EU in 2018 with special consideration given to interoperability issues, Int. J. Med. Inform. 141 (2020) 104205, https://doi.org/10.1016/j.ijmedinf.2020.104205.
[31] Docker, https://docs.docker.com/, 2024. (Accessed 15 October 2024).
[32] walt.id. Wallet kit, https://github.com/walt-id/waltid-walletkit, 2023. (Accessed 25 September 2023).
[33] NGINX, https://nginx.org/en/, 2024. (Accessed 15 October 2024).
[34] walt.id. REST APIs, https://docs.walt.id/v/web-wallet/getting-started/rest-apis, 2023. (Accessed 25 September 2023).
[35] Nuxt, Vue.js development, https://nuxt.com/docs/guide/concepts/vuejs-development, 2023. (Accessed 25 September 2023).
[36] walt.id. Web wallet, https://github.com/walt-id/waltid-web-wallet, 2023. (Accessed 25 September 2023).
[37] Metamask, A crypto wallet & gateway to blockchain apps, https://metamask.io/, 2023. (Accessed 25 September 2023).
[38] T. Hardin, D. Kotz, Amanuensis: information provenance for health-data systems, Inf. Process. Manag. 58 (2) (2021) 102460, https://doi.org/10.1016/j.ipm.2020.102460.
[39] H. Yin, S. Zhou, J. Jiang, Phala network: a secure decentralized cloud computing network based on Polkadot, https://api.semanticscholar.org/CorpusID:248089385, 2022. (Accessed 25 September 2023).
[40] O.T. Sam Curren, Tobias Looker, Didcomm messaging, https://identity.foundation/didcomm-messaging/spec/v2.1/, 2023. (Accessed 25 September 2023).
[41] C. Thatcher, S. Acharya, RxBlock: towards the design of a distributed immutable electronic prescription system, Netw. Model. Anal. Health Inf. Bioinform. 9 (1) (2020) 1–11, https://doi.org/10.1007/s13721-020-00264-5.
[42] P. Zhang, B. Stodghill, C. Pitt, et al., OpTrak: tracking opioid prescriptions via distributed ledger technology, Int. J. Inf. Syst. Soc. Change 10 (2) (2019) 45–61, https://doi.org/10.4018/IJISSC.2019040104.
[43] A. Taylor, A. Kugler, P.B. Marella, et al., VigilRx: a scalable and interoperable prescription management system using blockchain, IEEE Access 10 (2022) 25973–25986, https://doi.org/10.1109/ACCESS.2022.3156015.
[44] M.S. Islam, M.A.B. Ameedeen, H. Ajra, et al., Blockchain-enabled secure privacy-preserving system for public health-center data, Int. J. Adv. Comput. Sci. Appl. 14 (5) (2023) 1147–1154, https://doi.org/10.14569/ijacsa.2023.01405118.
[45] R.D. Garcia, G.S. Ramachandran, R. Jurdak, et al., A blockchain-based data governance with privacy and provenance: a case study for e-prescription, in: Proceedings of the 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2022, pp. 1–5, https://doi.org/10.1109/ICBC54727.2022.9805545.
[46] A.R. Lee, M.G. Kim, I.K. Kim, SHAREChain: healthcare data sharing framework using blockchain-registry and FHIR, in: Proceedings of the 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), IEEE, 2019, pp. 1087–1090, https://doi.org/10.1109/BIBM47256.2019.8983415.
[47] K. Kapadiya, U. Patel, R. Gupta, et al., Blockchain and AI-empowered healthcare insurance fraud detection: an analysis, architecture, and future prospects, IEEE Access 10 (2022) 79606–79627, https://doi.org/10.1109/ACCESS.2022.3194569.
[48] T.K. Mackey, K. Miyachi, D. Fung, et al., Combating health care fraud and abuse: conceptualization and prototyping study of a blockchain antifraud framework, J. Med. Internet Res. 22 (9) (2020) e18623, https://doi.org/10.2196/18623.
[49] L. Settipalli, G. Gangadharan, S. Bellamkonda, An extended lightweight blockchain based collaborative healthcare system for fraud prevention, Clust. Comput. 27 (1) (2023) 563–573, https://doi.org/10.1007/s10586-023-03973-4.
[50] L. Ismail, S. Zeadally, Healthcare insurance frauds: taxonomy and blockchain-based detection framework (Block-HI), IT Prof. 23 (4) (2021) 36–43, https://doi.org/10.1109/MITP.2021.3071534.
[51] G. Saldamli, V. Reddy, K.S. Bojja, et al., Health care insurance fraud detection using blockchain, in: Proceedings of the 2020 Seventh International Conference on Software Defined Systems (SDS), IEEE, 2020, pp. 145–152, https://doi.org/10.1109/SDS49854.2020.9143900.
[52] H.R. Hasan, K. Salah, R. Jayaraman, et al., Blockchain-based solution for COVID-19 digital medical passports and immunity certificates, IEEE Access 8 (2020) 222093–222108, https://doi.org/10.1109/ACCESS.2020.3043350.
[53] D.T. Harrell, M. Usman, L. Hanson, et al., Technical design and development of a self-sovereign identity management platform for patient-centric health care using blockchain technology, Blockchain Healthc. Today 5 (2022), https://doi.org/10.30953/bhty.v5.196.
[54] M. George, A.M. Chacko, Health passport: a blockchain-based PHR-integrated self-sovereign identity system, Front. Blockchain 6 (2023) 1075083, https://doi.org/10.3389/fbloc.2023.1075083.
[55] K. Leffew, Project Heisenberg, https://github.com/tylerdiaz/Heisenberg/blob/master/README.md, 2023. (Accessed 25 September 2023).
[56] M. Eisenstadt, M. Ramachandran, N. Chowdhury, et al., COVID-19 antibody test/vaccination certification: there's an app for that, IEEE Open J. Eng. Med. Biol. 1 (2020) 148–155, https://doi.org/10.1109/OJEMB.2020.2999214.