# ARTICLE      OPEN

# A blockchain-based framework to support pharmacogenetic data sharing

F. Albalwy [1,2,3 ✉], J. H. McDermott[4,5], W. G. Newman [4,5], A. Brass[1,3] and A. Davies[3]

The successful implementation of pharmacogenetics (PGx) into clinical practice requires patient genomic data to be shared between stakeholders in multiple settings. This creates a number of barriers to widespread adoption of PGx, including privacy concerns related to the storage and movement of identifiable genomic data. Informatic solutions that support secure and equitable data access for genomic data are therefore important to PGx. Here we propose a methodology that uses smart contracts implemented on a blockchain-based framework, PGxChain, to address this issue. The design requirements for PGxChain were identified through a systematic literature review, identifying technical challenges and barriers impeding the clinical implementation of pharmacogenomics. These requirements included security and privacy, accessibility, interoperability, traceability and legal compliance. A proof-of-concept implementation based on Ethereum was then developed that met the design requirements. PGxChain's performance was examined using Hyperledger Caliper for latency, throughput, and transaction success rate. The findings clearly indicate that blockchain technology offers considerable potential to advance pharmacogenetic data sharing, particularly with regard to PGx data security and privacy, large-scale accessibility of PGx data, PGx data interoperability between multiple health care providers and compliance with data-sharing laws and regulations.

## INTRODUCTION

It is a well-recognised clinical phenomenon that patients display variation in their response to medicines [1]. Such variation is regularly attributed to the chosen dosing strategy, the accuracy of the initial diagnosis or individual factors, such as comorbidities, polypharmacy, or compliance. However, there is increasing evidence that response to medicine is impacted by inherited genetic variation, a concept known as pharmacogenetics (PGx).

PGx dosing guidelines exist for many commonly prescribed medicines including antiplatelets, antidepressants, proton-pump inhibitors (PPIs), statins and anticoagulants [2–5]. Codeine, as an example, requires activation to morphine by the hepatic cytochrome P450 enzyme CYP2D6. Common genetic variants in the CYP2D6 gene impact the function of the CYP2D6 enzyme. Approximately 10% of the population are "poor" CYP2D6 metabolisers, meaning they fail to effectively convert codeine into morphine. Meanwhile, approximately 2% of individuals are ultra-rapid CYP2D6 metabolisers, in danger of producing high morphine levels, leading to toxicity. Despite this awareness, clinical implementation, especially in the UK, is limited to a few specific indications, namely the prescription of aminoglycosides [6], abacavir and fluoropyrimidine chemotherapy agents [5, 7, 8]. Current implementation typically involves a "reactive" testing strategy, where patients are tested for genetic variation relating to the medicine they are being prescribed at that moment in time.

A prospective testing approach, utilising PGx-specific genotyping panels containing variants related to the prescription of several medicines, represents an alternative strategy for clinical implementation [9–11]. Proponents of this approach cite the high prevalence of clinically relevant pharmacogenetic variants in the population and the widespread use of medicines for which pharmacogenetic dosing guidelines exist. Despite this, there are clearly barriers to prospective pharmacogenetic testing, as evidenced by the lack of clinical implementation across the UK. These barriers were recently discussed as part of a policy discussion, and the contributors highlighted a paucity of evidence around real-world clinical utility, the lack of intelligent decision support systems to aid implementation, and concerns around data security [9].

A prospective PGx strategy would involve genotype data from patients being stored in a repository, centralised or otherwise, where it can be accessed, and used to inform prescribing, as required. That may be several days after genotyping, or several years. Pharmacogenetic data, once available, remains relevant throughout an individual's life. As such, an informatic solution is required to store this data securely whilst allowing clinicians and patients access at relevant time points throughout their lives to inform safe and effective drug prescription. To address privacy concerns, any system should allow patients access to their own data, control over how that data is used, and oversight over who can access that data.

[1]Department of Computer Science, Kilburn Building, University of Manchester, Oxford Road, Manchester M13 9PL, UK. [2]Department of Computer Science, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia. [3]Division of Informatics, Imaging and Data Sciences, Stopford Building, University of Manchester, Oxford Road, Manchester M13 9PL, UK. [4]Manchester Centre for Genomic Medicine, St Mary's Hospital, Manchester University NHS Foundation Trust, Manchester M13 9WL, UK. [5]Division of Evolution Infection and Genomics, School of Biological Sciences, University of Manchester, Manchester, UK. ✉email: faisal.albalwy@manchester.ac.uk
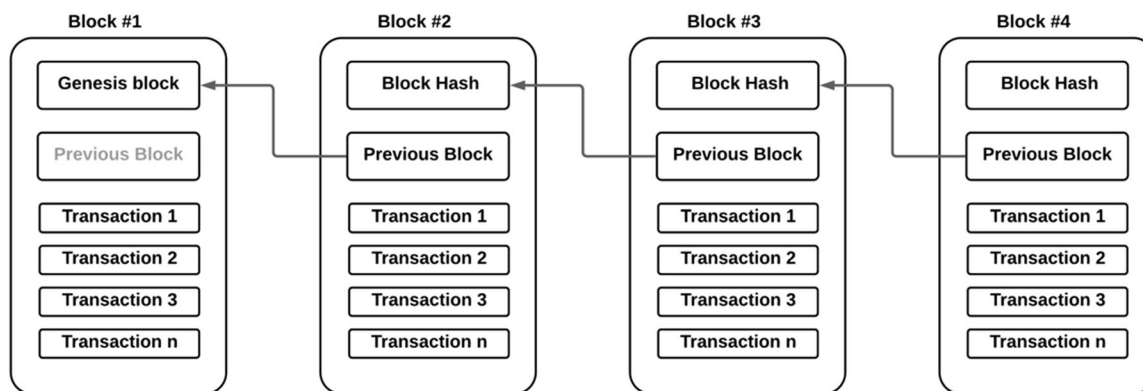
**Fig. 1 Simplified blockchain concept.** The structure of the blockchain is represented by a list of blocks where each block has specific transaction data and is linked to the previous block using the cryptographic hash of the previous block.

Any centralised informatic solution supporting PGx-guided prescribing would need the support of both clinical and public stakeholders. There exists a precedent for large-scale, seemingly well intentioned, national healthcare data data programmes failing because of confidentiality concerns. A high-profile example being the NHS England care.data programme which launched in 2013 and aimed to extract data from GP surgeries into a central database [12, 13]. Due to major privacy concerns and lack of public engagement, the programme was indefinitely suspended in 2016, and replaced in 2018 with the National data opt-out.

Effective and equitable pre-emptive PGx prescribing could necessitate the storage of genomic data in a centralised database which third-party electronic health record systems could interact with. This, however, raises privacy and security concerns as centralised databases lack transparency and accountability [14, 15]. Blockchain technology offers an immutable, transparent and accountable platform for storing PGx data that might address these concerns. Herein, we propose a blockchain-based framework to support PGx data sharing.

In the last decade, blockchain technology has attracted attention in academia and industry to explore its potential to combat data privacy concerns due to its transparency, accountability, and security features. Broadly speaking, blockchain is a type of secure database, called a shared ledger, distributed among multiple nodes within a peer-to-peer network. Each node in the network maintains an identical copy of the shared ledger. The ledger consists of a list of data structures called blocks. Each block contains transaction data (i.e. in this context, PGx data), a timestamp of its production and the cryptographic hash of the previous block, forming a chain of blocks (hence 'blockchain').

To append new data into the blockchain, new data are grouped into a new block, and then the network nodes use a consensus protocol, for example, a proof of work (PoW), to evaluate and verify the new block. The consensus protocol guarantees that new data are appended to the shared ledger only if most nodes validate the new block. Once a new block is appended to the shared ledger, it cannot be modified or removed, and since all nodes have an identical copy of the shared ledger, no node has the power to change the block data; hence, the shared ledger's integrity is ensured. Figure 1 illustrates a simplified blockchain concept.

Smart contracts are computer programmes that are stored and executed on the blockchain according to predefined conditions without the need for trusted intermediaries. Smart contracts were first introduced by Nick Szabo in the 1990s [16] and first implemented in 2014 in the Ethereum blockchain [17]. Here we propose a smart contract-based framework to facilitate secure PGx data sharing. To achieve this we have developed design requirements for such a system and implemented PGxChain, a proof-of-concept implementation for the proposed framework.

## MATERIALS/SUBJECTS AND METHODS
### Smart contracts
Smart contracts was first introduced by Nick Szabo in the 1990s a digital formalisation of a business relationship [16]. In blockchain, a smart contract is a computer programme that is stored, executed, and verified in the blockchain according to predefined conditions without the need for any trusted-third party [18]. The result of smart contract execution is a transaction recorded on a blockchain [19].

The primary purpose of smart contracts is to automatically execute agreements in response to the fulfilment of predefined conditions within the contract. The smart contract is executed when transactions are made, broadcast to the network and addressed to its addressed. Thus, a smart contract runs autonomously on every node across the blockchain network.

Thus, blockchains supporting smart contracts must allow for mutually distrustful counterparties to eliminate the possibility of dispute through engaging in a multi-step process. In this process, the transacting agents will be able to: (1): inspect the code prior to engaging with the contract to verify its outcomes; (2) achieve certainty of the execution of the code (which is possible due to the decentralised nature of the network upon which the code is deployed, with no single actor able to direct the entire process); and (3) verify the entire smart contract process (which is possible due to the digital signatures involved in the process). As participants cannot disagree over the result of this verifiable process, the possibility for dispute and asynchrony is eliminated.

Smart contracts are, in effect, autonomous agents; their behaviour is pre-determined by the code governing them. Because of this, provided the data they are required to manage is within their parameters, they are trusted to carry out any computational logic inscribed upon the chain and expressed as a function of on-chain data inputs.

Across different blockchain platforms, smart contracts are developed and deployed to various ends. The programming language supported by each blockchain varies, with Ethereum allowing for the execution of advanced, customised smart contracts through high-level programming languages such as Solidity and Vyper [20].

### Establishing system design requirements
To identify the design requirements for the proposed solution, we used PRISMA guidelines to conduct a Systematic Literature Review (SLR) [21] and analysed the existing literature concerning technical challenges and barriers impeding the implementation of pharmacogenomics.

The SLR accessed articles published between 1 January 2015 up to 5 July 2021. Four databases, namely PubMed, Scopus, IEEE

**Fig. 2  Research query.** The search terms used to search databases including PubMed, Scopus, IEEE Explore and Web of Science.

Explore and Web of Science were queried using the search query shown in Fig. 2. The resulting articles were imported to Covidence, an online application tool used to manage systematic reviews. Duplicate articles were removed and articles were screened by the authors, and articles that did not include pharmacogenomics clinical implementation challenges were excluded. Articles were then assessed by the authors for eligibility, using the following exclusion criteria:

- No technical challenges and barriers provided
- No access to the full text
- Non-English language article
- Review article

Section "Identified system design requirements" shows the results of the search procedure.

### Design science research
We applied a design science research (DSR) methodology [22] to develop and evaluate a blockchain-based system to meet the identified design requirements. The DSR provides guidelines and principles to address problems through the creation of innovative IT artefacts. The DSR consists of six elements: problem identification and motivation, objectives of the solution, design of the solution, development of the solution, evaluation of the solution and research communications (Fig. 3).

### System architecture
The proposed blockchain-based system for supporting PGx data storage and sharing contains several discrete architecture components; users, on-chain resources and off-chain resources (Fig. 1 in Appendix 2):

- Users.
    Data creator – an organisational entity, such as a genomic laboratory hub, where PGx data are sequenced and stored. Patient – an individual whose PGx data are stored in a secure storage space managed by the data creator. Data requester – a healthcare professional (e.g. pharmacist, physician) who needs access to patient's PGx data in a clinical situations.

- On-chain resources
    Smart contracts – these are used to provide system functionalities, such as user management and data access management.
    Logs and events – these are created by smart contracts for all system transactions. Logs and events are stored on-chain, and they are critical for tracing and auditing all system actions, thus making system users accountable for their transactions.

- Off-chain resources
    Secure storage – a private secure database managed by a data creator that contains the patient's PGx data.
    Oracle server – a trusted data feed service that provides off-chain data to the blockchain. This is an important component as blockchain and smart contracts by design cannot access and read off-chain data.
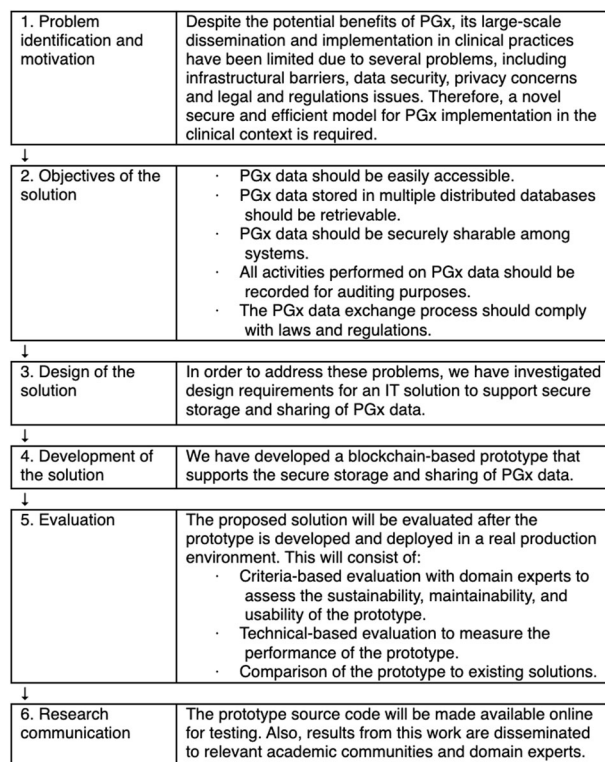
| 1. Problem identification and motivation | Despite the potential benefits of PGx, its large-scale dissemination and implementation in clinical practices have been limited due to several problems, including infrastructural barriers, data security, privacy concerns and legal and regulations issues. Therefore, a novel secure and efficient model for PGx implementation in the clinical context is required. |
|---|---|
| 2. Objectives of the solution | · PGx data should be easily accessible.<br>· PGx data stored in multiple distributed databases should be retrievable.<br>· PGx data should be securely sharable among systems.<br>· All activities performed on PGx data should be recorded for auditing purposes.<br>· The PGx data exchange process should comply with laws and regulations. |
| 3. Design of the solution | In order to address these problems, we have investigated design requirements for an IT solution to support secure storage and sharing of PGx data. |
| 4. Development of the solution | We have developed a blockchain-based prototype that supports the secure storage and sharing of PGx data. |
| 5. Evaluation | The proposed solution will be evaluated after the prototype is developed and deployed in a real production environment. This will consist of:<br>· Criteria-based evaluation with domain experts to assess the sustainability, maintainability, and usability of the prototype.<br>· Technical-based evaluation to measure the performance of the prototype.<br>· Comparison of the prototype to existing solutions. |
| 6. Research communication | The prototype source code will be made available online for testing. Also, results from this work are disseminated to relevant academic communities and domain experts. |

**Fig. 3  The DSR's elements.** The Design Science Research Model employed in this research work.
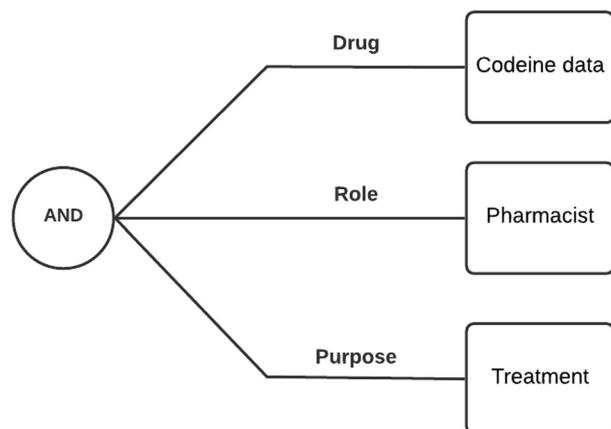
### Smart contracts
Three smart contracts were written to provide system functionalities: a registration smart contract (RSC), a data smart contract (DSC) and an access control manager smart contract (ACMSC). Table 1 shows the system's smart contracts main functions.

*Registration smart contract (RSC).* To interact with the system, each user must register through a registration smart contract. The registration is an invitation-based process where the system owner, who is responsible for setting up the system e.g National Health Service (NHS), invites users to join the system. During the registration process, users' identities and professional registrations should be verified by the system owner. The verification process is an off-chain process and requires using external trusted sources of information such as GOV.UK Verify and NHS Identity. Section 1.1 in Appendix 2 describes the user registration process for the patient, data creator and data requestor, respectively.

*Data smart contract (PDSC).* This smart contract is responsible for the process of submitting patients' PGx metadata data to the system. After collecting and storing patients' PGx data in secure, off-chain storage, the data creator submits the patients' PGx metadata data, which includes a description of the patients' data that does not reveal sensitive information, to the system by executing the *createData* function. This PGx metadata includes a list pre-defined medicines for which gene-drug guidelines exist and the corresponding prescribing recommendations based on the patient's pharmacogenetic results. This metadata serves two goals: first, to reference the original data stored off-chain within data creator's secure storage and second, to ensure the integrity of patients' PGx data stored off-chain. Section 1.2 in Appendix 2 describes the process of submitting patients' PGx metadata data to the system.

**Table 1.** System's smart contracts main functions.

| # | Function | Descriptions |
|---|----------|--------------|
| 1 | *patientRegister* | Responsible for the registration process for patient |
| 2 | *dataRequesterRegister* | Responsible for the registration process for data requester |
| 3 | *dataCreatorRegister* | Responsible for the registration process for data creator |
| 4 | *createData* | Responsible for the process of submitting patient's PGx metadata data to the system |
| 5 | *requestAccessTicket* | Responsible for managing access to patient's PGx data |
| 6 | *requestAccessToken* | Responsible for minimising access to patient's PGx data |
| 7 | *setAcessPermission* | Responsible for granting access to patient's PGx data |
| 8 | *cancelAcessPermission* | Responsible for revoking access for patient's PGx data |



**Fig. 4 An example of Patients' permission elements.** In this example, Patients' permission elements are represented by a decision tree where patient codeine data can be accessed by a pharmacist for treatment.

**Table 2.** Configurations of Go-ethereum and the testing environment.

| Factor | Setting |
|--------|---------|
| Nodes | Four VMs running ubuntu 20.04 on Microsoft Azure cloud, where each VM has 2 Intel CPU and 8 GB. |
| Peer-to-Peer Network | Go-ethereum v1.10.11 |
| | 1 validator node |
| | 3 peer nodes |
| Consensus Protocol | Clique |
| Smart Contracts | Solidity |
| Benchmarking Tool | Hyperledger Caliper v0.4.2 |

*Access control manager smart contract (ACMSC).* This smart contract is responsible for managing access to the PGx data through four functions, namely *setAcessPermission*, *cancelAcessPermission*, *requestAccessTicket* and *requestAccessToken*.

The *setAcessPermission* function defines the patient's permissions preferences for accessing their PGx data. Patients' permission preferences are defined by specifying three elements: drug name, the role of who needs access to patient PGx data and the purpose of the access to patient PGx data. Tables 2A, 2B and 2C in Appendix 2 show an abstract view of the patient's permission preferences elements and their codes. These elements are then represented by a decision tree which provides a Boolean formula that represents the patient's permission preferences (Fig. 4). An access request for patient PGx data is considered valid only if it satisfies the tree logic. Section 1.3 in Appendix 2 describes the process of managing the patient's permission preferences in the smart contract and the process of managing access to patient's data.

**Performance evaluation environment**
To evaluate the performance of proposed system, we used four virtual machines (VMs) running on Microsoft Azure (https://azure.microsoft.com/) cloud to build a private blockchain utilising Go-ethereum (https://geth.ethereum.org/), an open-source Ethereum client that provides permissioned private blockchain networks. We also used Hyperledger Caliper (https://www.hyperledger.org/use/caliper), an open-source benchmarking tool for investigating the performance of blockchain applications, to perform multiple tests to validate the system performance. Table 2 shows the configurations of the private blockchain and the testing environment. Two main types of blockchain

operations, *Write* and *Read* operations, were tested using five performance metrics to evaluate the proposed system: *Write* throughput, *Read* throughput, *Write* latency, *Read* latency and scalability. Figures 5 and 6 summarise the parameters used for evaluating the Write and Read operations, respectively.

To help identify the system scalability threshold, we conducted an additional test using a linear transaction to send several transactions to the blockchain. Figure 7 summarises the parameters used to evaluate the system scalability.

**RESULTS**
**Identified system design requirements**
The flow of the systematic review is shown in Fig. 8. The articles retrieved from the initial search ($N = 723$) were imported to Covidence. Duplicate articles ($n = 365$) were removed and each articles' abstract ($n = 358$) was screened by the authors to remove out-of-scope articles ($n = 228$). Full-text articles ($n = 130$) were then assessed by the authors for eligibility (as described in section 2.1). The resulting articles ($n = 33$) were reviewed and data extracted. The final findings are summarised in Table 3.

**A proof of concept**
To demonstrate feasibility of the proposed blockchain-based architecture, we implemented PGxChain. Go-ethereum (https://geth.ethereum.org/), an open-source Ethereum client, was used as a permissioned blockchain to host PGxChain. The Solidity programming language was used to write the system smart contracts. The truffle framework, an Ethereum smart contracts development tool was used to test, compile and deploy system smart contracts. Finally, we utilised Node.js and MongoDB to develop and build the off-chain resources. A demonstration video has been uploaded to show the proof-of-concept implementation (https://youtu.be/E13AP-1hDDQ).

PGxChain provides a prototype web portal for system users to interact with the system. It enables patients to grant or revoke their permissions regarding the sharing of their PGx data. It also allows

```
 1  test:
 2    name: Write performance
 3    description:
      This is a benchmark for caliper, to test the backend  smart
      contract's Read performance
 4    workers:
 5      type: local
 6      number: 5
 7    rounds:
 8      - label: 50TSP
 9        txNumber: 1000
10        rateControl: { type: fixed-rate, opts: { tps: 10 } }
11        callback: benchmarks/callbacks/Write.js
12      - label: 10TSP
13        txNumber: 1000
14        rateControl: { type: fixed-rate, opts: { tps: 110 } }
15        callback: benchmarks/callbacks/Write.js
16      - label: 15TSP
17        txNumber: 1000
18        rateControl: { type: fixed-rate, opts: { tps: 210 } }
19        callback: benchmarks/callbacks/Write.js
20      - label: 20TSP
21        txNumber: 1000
22        rateControl: { type: fixed-rate, opts: { tps: 310 } }
23        callback: benchmarks/callbacks/Write.js
24      - label: 25TSP
25        txNumber: 1000
26        rateControl: { type: fixed-rate, opts: { tps: 410 } }
27        callback: benchmarks/callbacks/Write.js
28      - label: 30TSP
29        txNumber: 1000
30        rateControl: { type: fixed-rate, opts: { tps: 510 } }
31        callback: benchmarks/callbacks/Write.js
32      - label: 35TSP
33        txNumber: 1000
34        rateControl: { type: fixed-rate, opts: { tps: 610 } }
35        callback: benchmarks/callbacks/Write.js
36      - label: 40TSP
37        txNumber: 1000
38        rateControl: { type: fixed-rate, opts: { tps: 710 } }
39        callback: benchmarks/callbacks/Write.js
40      - label: 45TSP
41        txNumber: 1000
42        rateControl: { type: fixed-rate, opts: { tps: 810 } }
43        callback: benchmarks/callbacks/Write.js
44      - label: 50TSP
45        txNumber: 1000
46        rateControl: { type: fixed-rate, opts: { tps: 910 } }
47        callback: benchmarks/callbacks/Write.js
48      - label: 50TSP
49        txNumber: 1000
50        rateControl: { type: fixed-rate, opts: { tps: 1010
      } }
51        callback: benchmarks/callbacks/Write.js
52  monitor:
53    type:
54      - none
```

**Fig. 5 Experimental settings for Write operations.** These settings are related to the benchmark configuration workload for Write operations.

data creators to store patients' PGx data and data requesters to access patients' PGx data. Figure 2 in Appendix 2 shows the dataRequester web portal interface provided by PGxChain. The high-level structure and workflow are detailed in Fig. 9.

**Performance evaluation**
The results of the *Write* and *Read* operations indicated an average *Write* throughput of 90.51 tps (Fig. 4 in Appendix 1) and an average *Read* throughput of 103.38 tps (Fig. 5 in Appendix 1).

```
 1  test:
 2    name: Read performance
 3    description:
      This is a benchmark for caliper, to test the backend  smart
      contract's Read performance
 4    workers:
 5      type: local
 6      number: 1
 7    rounds:
 8      - label: 10TSP
 9        txNumber: 1000
10        rateControl: { type: fixed-rate, opts: { tps: 10 } }
11        callback: benchmarks/callbacks/Read.js
12      - label: 110TSP
13        txNumber: 1000
14        rateControl: { type: fixed-rate, opts: { tps: 110 } }
15        callback: benchmarks/callbacks/Read.js
16      - label: 210TSP
17        txNumber: 1000
18        rateControl: { type: fixed-rate, opts: { tps: 210 } }
19        callback: benchmarks/callbacks/Read.js
20      - label: 310TSP
21        txNumber: 1000
22        rateControl: { type: fixed-rate, opts: { tps: 310 } }
23        callback: benchmarks/callbacks/Read.js
24      - label: 410TSP
25        txNumber: 1000
26        rateControl: { type: fixed-rate, opts: { tps: 410 } }
27        callback: benchmarks/callbacks/Read.js
28      - label: 510TSP
29        txNumber: 1000
30        rateControl: { type: fixed-rate, opts: { tps: 510 } }
31        callback: benchmarks/callbacks/Read.js
32      - label: 610TSP
33        txNumber: 1000
34        rateControl: { type: fixed-rate, opts: { tps: 610 } }
35        callback: benchmarks/callbacks/Read.js
36      - label: 710TSP
37        txNumber: 1000
38        rateControl: { type: fixed-rate, opts: { tps: 710 } }
39        callback: benchmarks/callbacks/Read.js
40      - label: 810TSP
41        txNumber: 1000
42        rateControl: { type: fixed-rate, opts: { tps: 810 } }
43        callback: benchmarks/callbacks/Read.js
44      - label: 910TSP
45        txNumber: 1000
46        rateControl: { type: fixed-rate, opts: { tps: 910 } }
47        callback: benchmarks/callbacks/Read.js
48      - label: 1010TSP
49        txNumber: 1000
50        rateControl: { type: fixed-rate, opts: { tps: 1010
      } }
51        callback: benchmarks/callbacks/Read.js
52    monitor:
53      type:
54        - none
```

**Fig. 6  Experimental settings for Read operations.** These settings are related to the benchmark configuration workload for Read operations.

The *Write* latency was 5.49 seconds (Fig. 6 in Appendix 1), whereas the average *Read* latency was 4.86 s (Fig. 7 in Appendix 1). Moreover, the system performance analysis (Fig. 8 in Appendix 1) revealed that a large number of *R*ead operations (i.e. 10,000 transactions) could be handled by PGxChain with very low latency, whereas *Write* operations are processed with higher latency due to the complexity involved in writing to the blockchain network.

```
1  test:
2    name: Scalability Test
3    description:
     This is a benchmark for caliper, to test the PGxChain scalability
4    workers:
5      type: local
6      number: 5
7    rounds:
8      - label: Tx100Read
9        txNumber: 100
10       rateControl: { type: fixed-rate, opts: { tps: 100 } }
11       callback: benchmarks/callbacks/Read.js
12     - label: Tx1000Read
13       txNumber: 1000
14       rateControl: { type: fixed-rate, opts: { tps: 100 } }
15       callback: benchmarks/callbacks/Read.js
16     - label: Tx10000Read
17       txNumber: 10000
18       rateControl: { type: fixed-rate, opts: { tps: 100 } }
19       callback: benchmarks/callbacks/Read.js
20     - label: Tx100Write
21       txNumber: 100
22       rateControl: { type: fixed-rate, opts: { tps: 100 } }
23       callback: benchmarks/callbacks/Write.js
24     - label: Tx1000Write
25       txNumber: 1000
26       rateControl: { type: fixed-rate, opts: { tps: 100 } }
27       callback: benchmarks/callbacks/Write.js
28     - label: Tx10000Write
29       txNumber: 10000
30       callback: benchmarks/callbacks/Write.js
31   monitor:
32     type:
33       - none
```

**Fig. 7 Experimental settings for system scalability evaluation.** These settings are related to the benchmark configuration workload for testing the system scalability.
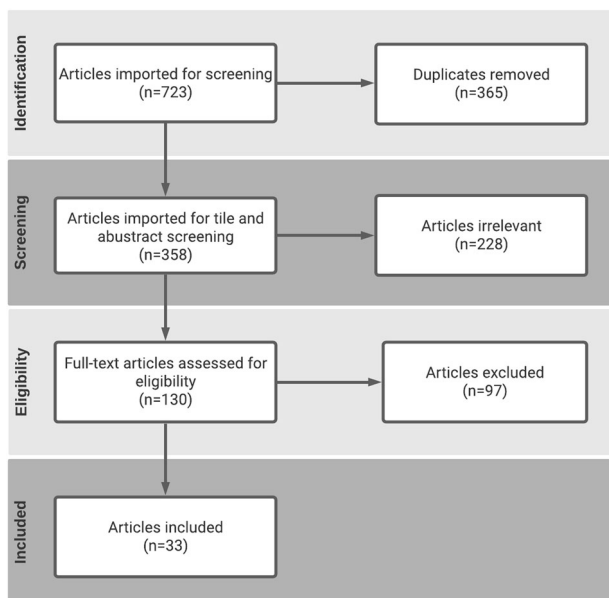


**Fig. 8 PRISMA flow diagram.** The flow of information through the different phases of this review (number of records identified, excluded, and included).

## DISCUSSION
### Addressing requirement
PGxChain offers a mechanism for sharing of pharmacogenetic data between stakeholders in a secure and equitable way, but to what extent does it meet the design requirements as defined in Table 2?

*R1: security and privacy.* Implementing PGx in clinical practice will require the movement and sharing of genetic data across traditional institutional boundaries. PGxChain preserves privacy by utilising a permissioned blockchain and pseudo-anonymous accounts that represent users' identities. Authorised users can only access PGxChain through their pseudo-anonymous accounts, allowing them to interact with the system by submitting transactions to the blockchain without revealing their real identities. In addition, users can create multiple pseudo-anonymous accounts. Hence, user transactions cannot be inferred by an adversary.

In PGxChain, data security is maintained through the use of a hybrid data storage model that includes on-chain/off-chain storage. In this model, PGx data are stored securely off-chain, and only PGx metadata are submitted to the blockchain. PGx metadata include non-identifiable information, such as drug name, a hash value of off-chain PGx data to ensure data integrity and a reference pointer to the off-chain PGx data secured by public-key cryptography. Moreover, to reduce the risk of data breaches or leaks, PGxChain uses a one-time access-token, whereby authorised users can access requested PGx data within

**Table 3.** Identified system design requirements.

| # | Identified design requirements | Barriers and challenges | Studies |
|---|---|---|---|
| R1 | Security and privacy | • Secure storage of the PGx data<br>• Unauthorised access to PGx data<br>• Preserving patient privacy and confidentiality when outsourceing data | [29–47] |
| R2 | Accessibility | • Limited data sharing<br>• Time lag to receive the results<br>• Lack of infrastructure and standardised processes for storing, accessing PGx data<br>• And reporting results efficiently<br>• Communicate results to patients | [29, 40, 43, 44, 48–59] |
| R2 | Interoperability | • Difficulties of integrating PGx data with the EHR<br>• Low degree of connectivity between different PGx resources<br>• Lack of a link between several software-systems<br>• Integrating PGx testing into existing services | [29, 43, 45–48, 50, 52–55, 58–61] |
| R4 | Traceability | • Lack of transparency<br>• Uncertainty of about the appropriate level of oversight<br>• Lack of patient engagement in care decision making<br>• Future use of patient PGx data<br>• Who could have access to PGx data? | [42, 44, 59, 61, 62] |
| R5 | Legal Compliance | • Autonomy and informed consent issues<br>• Risk of discrimination<br>• Misuse of patient data<br>• Legal uncertainty<br>• Lack of accountability regarding PGx data ownership | [30, 33, 35–38, 50, 61, 63] |
| # | Identified design requirements | Barriers and challenges | Studies |
| R1 | Security and privacy | • Secure storage of the PGx data<br>• Unauthorised access to PGx data<br>• Preserving patient privacy and confidentiality when outsourceing data | [29–47] |
| R2 | Accessibility | • Limited data sharing<br>• Time lag to receive the results<br>• Lack of infrastructure and standardised processes for storing, accessing PGx data<br>• And reporting results efficiently<br>• Communicate results to patients | [29, 31, 34, 35, 48–59] |
| R2 | Interoperability | • Difficulties of integrating PGx data with the EHR<br>• Low degree of connectivity between different PGx resources<br>• Lack of a link between several software-systems<br>• Integrating PGx testing into existing services | [29, 34, 36–38, 48, 49, 52–54, 56, 58–61] |
| R4 | Traceability | • Lack of transparency<br>• Uncertainty of about the appropriate level of oversight<br>• Lack of patient engagement in care decision making<br>• Future use of patient PGx data<br>• Who could have access to PGx data? | [33, 35, 53, 61, 62] |
| R5 | Legal compliance | • Autonomy and informed consent issues<br>• Risk of discrimination<br>• Misuse of patient data<br>• Legal uncertainty<br>• Lack of accountability regarding PGx data ownership | [30, 41, 43–46, 56, 61, 63] |

a given time frame. Due to the one-time access token and public-key cryptography, a compromised reference pointer to PGx data is useless and will not lead to data leakage.

*R2: Accessibility.* Genomic data, including PGx data, carry notable characteristics that make it different from other health data. PGxChain leverages smart contracts as well as the one-time access token to achieve a balance between the privacy and accessibility of PGx data. The smart contracts are used to manage patients' permissions, enabling patients to amend or delete their permissions as they desire at any time, and these changes are reflected in the system immediately. The secure one-time access token ensures that only authorised data requesters can access PGx data within a given time frame. Consequently, the accessibility of PGx data is maximised while data privacy is preserved.

*R3: Interoperability.* PGxChain leverages blockchain features, including transparency and accountability, to present a modular model design that can be integrated with health care providers' existing systems to foster responsible PGx data sharing. This could promote PGx data interoperability across health care systems, allowing applications such as clinical decision support (CDS) to use PGx data along with electronic health records (EHRs) effectively in the clinical practice context.
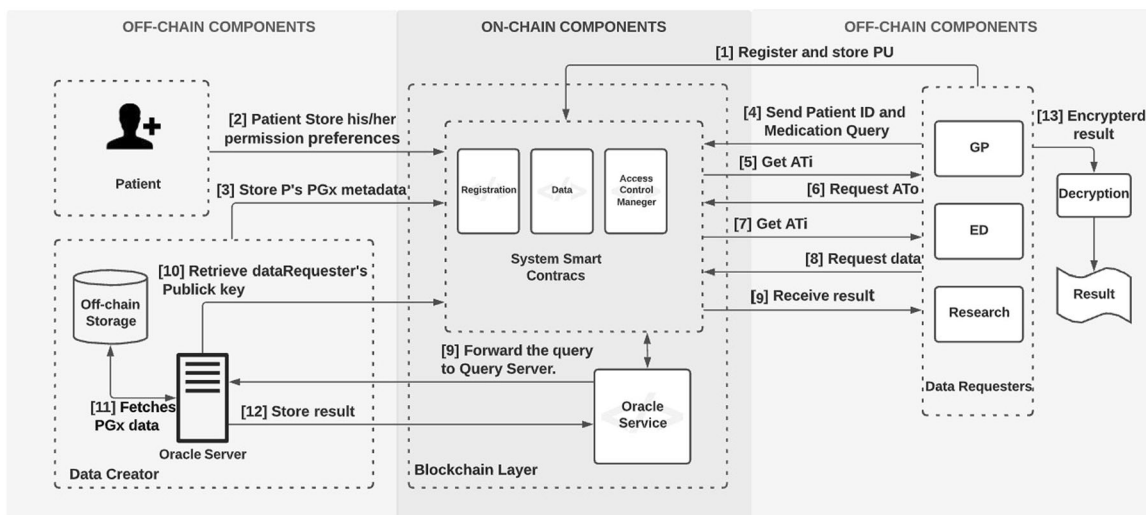
**Fig. 9 The high-level structure and workflow of PGxChain.** The high-level structure and workflow of PGxChain. The workflow includes the following steps: [1] During the registration, data requester generates a pair of keys: public (PU) and private (PR). Data requester then stores PU in RSC. [2] Patient stores their permission preferences (drug, role and purpose) in ACMSC. [3] Data creator collects patient's PGx data and stores it in a secure, off-chain database and stores patient's PGx metadata in DSC. [4,5] Data requester request Access Ticket (ATi) by specifying a patient ID, medication query and purpose for accessing data. The request is accepted or rejected automatically based upon patient permission preferences stored in ACMSC. Upon accepted request, an ATi is generated and stored in ACMSC. [6,7] Data requester sends ATi to ACMSC to request Access Token (ATo). The request is accepted or rejected automatically based upon ATi validation. Upon acceptance of the request, the ATo is generated and stored in ACMSC. [8,9] Data requester sends ATo to ACMSC in order to retrieve patient's PGx data stored in the off-chain database. The request is accepted or rejected automatically based upon ATo validation. Upon acceptance, the request is forwarded to Oracle Server (OS). [10] OS retrieves the data requester's PU from RSC. [11] OS fetches patient's PGx data from the database and creates a temporary JSON file that contains patients' data. This JSON file can be accessed via HTTPS requests only for one-time access. [12] OS encrypts the URL for JSON file using data requester's PU and stores the encrypted URL (eURL) in ACMSC. [13] Data requester retrieves eURL from ACMSC and decrypts it using the corresponding PR in order to access the JSON file.

*R4: Data control and traceability.* PGxChain manages the sharing of PGx data using smart contracts. Therefore, all system processes and actions are recorded permanently on the blockchain, providing an immutable log of all system transactions. This enables patients to inspect the blockchain to learn more about their PGx data and where their PGx data are stored off-chain, who has access to them and for what purpose. In addition, PGxChain enables data creators to update information related to variables' responses to new drugs as there are discovered which enables data requesters to query up-to-date drug metadata stored on-chain. This is a significant feature as the pathogenic significance of genetic variants might be changed as clinical research advances. Moreover, access to an immutable log of all system transactions would enable regulators to investigate claims in the event of disputes or trangressions.

*R5: Legal compliance.* The compliance of blockchains with legal regulations is an area of debate. For example, in the General Data Protection Regulation (GDPR), although a blockchain can help to comply with Article 7 (Conditions for Consent), it seems to be in conflict with Article 17 (right to erasure). Therefore, it is not possible to determine whether blockchains are completely compliant or non-compliant with the GDPR [23]. To reconcile blockchain-based applications with the GDPR, such legal regulations should be taken into account during the design decision stage. In PGxChain, the use of smart contracts to manage patient permissions enables patients to grant and revoke access to their PGx data, shifting data control from institutions to the patients. This supports patient-centric approaches to managing consent, providing patients with more control of their PGx data, thus complying with Article 7 of the GDPR. In addition, to comply with Article 14 of the GDPR, PGxChain adopts a hybrid data storage model that stores patients' PGx data in secure off-chain storage from which data can be removed. Only PGx metadata, which contain non-identifiable information as well as a secure reference

pointer to the original PGx data, are stored on the blockchain. In the event a patient requests the removal of their PGx data from the system, their PGx data can be removed from the off-chain storage. As suggested by the GDPR, to optimise data privacy while minimising data storage and access, PGxChain only stores patients' PGx metadata on the blockchain and utilises a one-time access token to reduce access to PGx data.

### Comparison with existing systems

Several systems have been previously developed to manage PGx data. Dolin et al. [24] demonstrated a functional prototype for CDS that can be used in clinical pharmacogenomics, where clinicians can query relevant genetic data in a Genomic Archiving and Communication System (GACS). Danahey et al. [25] designed and implemented a Genomic Prescribing System (GPS) to manage PGx data, which provides drug-variant-specific clinical decision support summaries. John et al. [26] presented a web-based pharmacogenomics tool called PharmaKU, which extracts variants from nine well-annotated pharmacogenes from individual WGS VCF files and reports the results in a comprehensive PDF document. Linderman et al. [27] developed a privacy-preserving web application called MySeq for interactive personal genome analysis including PGx, in which genotypes and associated phenotypes based on the drug labels for simvastatin and warfarin are reported. At the 2019 iDASH (Integrating Data for Analysis, Anonymization, and Sharing) competition, as part of the Secure Genome Analysis challenge, Gürsoy et al. [28] proposed a blockchain-based solution to efficiently store and query PGx data on the Ethereum blockchain.

However, all the systems mentioned earlier, except Gürsoy et al. [28], are centralised systems developed using centralised architecture models limiting access to PGx data due to privacy and security concerns. The blockchain-based solution proposed by Gürsoy et al. handles storing and querying PGx data on the Ethereum blockchain and protects data from loss in a single point

**Table 4.** A comparison between existing systems and PGxChain.

| Reference | System design requirements | | | | | Blockchain-based? | System evaluated? |
|---|---|---|---|---|---|---|---|
| | R1 | R2 | R3 | R4 | R5 | | |
| CDS Hooks [24] | Y | Y | Y | N | N | N | N |
| Genomic Prescribing System (GPS) [25] | Y | Y | Y | N | N | N | N |
| PharmaKU [26] | Y | Y | N | N | N | N | N |
| MySeq [27] | N | Y | N | N | N | N | N |
| Gürsoy et al. [28] | Y | Y | N | N | N | Y | Y |
| PGxChain | Y | Y | Y | Y | Y | Y | Y |

R1: Security and Privacy R2: Accessibility R3: Interoperability R4: Traceability R5: Legal compliance.

of failure scenario or accidental or intentional corruption. However, it does not address other issues such as secure storage of the PGx data, unauthorised access to PGx data and consent issues. Table 4 presents a comparison between existing systems and PgxChain.

## Limitations
Owing to the openness and to the distributed nature of blockchain technology, verifying user identity is challenging. Our proposed framework assumes that PGxChain operates in a private blockchain and that all users are invited to join the system. As such, users' identity verification will be performed before they join the system, and users will be given pseudonymous identifiers to represent them in the system. A more reliable and practical solution to overcome this limitation is to integrate the system with an identity management service, such as GOV.UK Verify or NHS Identity.

Yet another limitation is that vulnerable patients might not possess the necessary ICT skills to manage their consent preferences. The current implementation of blockchain and smart contracts technologies requires some software/hardware prerequisites to interact with the system (i.e soft/hard wallets), which might be available only in a limited number of operating systems and internet browsers.

## CONCLUSION
Several barriers, including concerns about data security and privacy, are contributing to the delays in clinical implementation of PGx on a large scale. In this article, we proposed a blockchain-based framework for PGx data sharing. We provide a proof-of-concept implementation, PGxChain, which was implemented on a private Ethereum blockchain. The proposed framework achieved large-scale sharing of PGx data among the involved stakeholders. Prior to wider deployment of the system, user-focus groups will be critical to optimise the user-interface, ensuring that individuals with a broad range of IT skills are able to interact with the system equitably. PGx data was chosen as an exemplar, though the system could reasonably be adapted for other types of data where required. The performance analysis showed that the system is efficient and scalable. The potential of PGxChain for supporting the sharing of both PGx and medical data is promising.

## DATA AVAILABILITY
All data used in the framework are available from the corresponding author on reasonable request.

## REFERENCES
1. Roden DM, Wilke RA, Kroemer HK, Stein CM. Pharmacogenomics: the genetics of variable drug responses. Circulation. 2011;123:1661–70.
2. Scott SA, Sangkuhl K, Stein CM, Hulot JS, Mega JL, Roden DM, et al. Clinical pharmacogenetics implementation consortium guidelines for CYP2C19 genotype and clopidogrel therapy: 2013 update. Clin Pharmacol Ther. 2013;94:317–23.
3. Lima JJ, Thomas CD, Barbarino J, Desta Z, Van Driest SL, El, et al. Clinical Pharmacogenetics Implementation Consortium (CPIC) guideline for CYP2C19 and proton pump inhibitor dosing. Clin Pharmacol Ther. 2021;109:1417–23.
4. Wilke RA, Ramsey LB, Johnson SG, Maxwell WD, McLeod HL, Voora D, et al. The clinical pharmacogenomics implementation consortium: CPIC guideline for SLCO1B1 and simvastatin-induced myopathy. Clin Pharmacol Ther. 2012;92:112–7.
5. Martin MA, Klein TE, Dong BJ, Pirmohamed M, Haas DW, Kroetz DL. Clinical pharmacogenetics implementation consortium guidelines for HLA-B genotype and abacavir dosing. Clin Pharmacol Ther. 2012;91:734–8.
6. McDermott JH, Mahaveer A, James RA, Booth N, Turner M, Harvey KE, et al. Rapid point-of-care genotyping to avoid aminoglycoside-induced ototoxicity in neonatal intensive care. JAMA Pediatr. 2022;176:486. https://jamanetwork.com/journals/jamapediatrics/fullarticle/2790066
7. Payne K, Fargher EA, Roberts SA, Tricker K, Elliott RA, Ratcliffe J, et al. Valuing pharmacogenetic testing services: A comparison of patients' and health care professionals' preferences. Value Health. 2011;14:121–34.
8. Medicines and Healthcare Products Regulatory Agency. 5-fluorouracil (intravenous), capecitabine, tegafur: DPD testing recommended before initiation to identify patients at increased risk of severe and fatal toxicity. Gov.uk. 2020. https://www.gov.uk/drug-safety-update/5-fluorouracil-intravenous-capecitabine-tegafur-dpd-testing-recommended-before-initiation-to-identify-patients-at-increased-risk-of-severe-and-fatal-toxicity#characteristics
9. Turner RM, Newman WG, Bramon E, McNamee CJ, Wong WL, Misbah S, et al. Pharmacogenomics in the UK National Health Service: opportunities and challenges. Pharmacogenomics 2020;21:1237–46.
10. Roden DM, McLeod HL, Relling MV, Williams MS, Mensah GA, Peterson JF, et al. Pharmacogenomics. Lancet. 2019;394:521–32.
11. Weitzel KW, Cavallari LH, Lesko LJ. Preemptive panel-based pharmacogenetic testing: the time is now. Pharm Res. 2017;34:1551–5.
12. Hoeksma J. The NHS's care.data scheme: what are the risks to privacy? BMJ. 2014;348:g1547–g1547.
13. McCartney M. Care.data doesn't care enough about consent. BMJ. 2014;348:g2831–g2831.
14. Thorisson GA, Muilu J, Brookes AJ. Genotype-phenotype databases: challenges and solutions for the post-genomic era. Nat Rev Genet. 2009;10:9–18.
15. Chaterji S, Koo J, Li N, Meyer F, Grama A, Bagchi S. Federation in genomics pipelines: techniques and challenges. Brief Bioinform. 2019;1:235–44.
16. Szabo N. Formalizing and securing relationships on public networks. First Monday. 1997. http://journals.uic.edu/ojs/index.php/fm/article/view/548
17. Buterin V. Ethereum white paper: a next generation smart contract & decentralized application platform. Etherum. 2014. https://translatewhitepaper.com/wp-content/uploads/2021/04/EthereumOrijinal-ETH-English.pdf
18. Cannarsa M. Interpretation of contracts and smart contracts: smart interpretation or interpretation of smart contracts? Eur Rev Priv Law. 2018;26:773–85.
19. Buterin V. A next-generation smart contract and decentralized application platform. 3, Etherum. 2014. p. 1–36. http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf
20. Delmolino K, Arnett M, Kosba A, Miller A, Shi E. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In International conference on financial cryptography and data security. Berlin, Heidelberg: Springer; 2016, pp. 79–94.
21. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ. 2021. p. n71. https://www.bmj.com/lookup/doi/10.1136/bmj.n71

22. Hevner A, Chatterjee S. Design science research in information systems. In: Design research in information systems. Springer; 2010. p. 9–22. http://link.springer.com/10.1007/978-1-4419-5653-8_2

23. Wohlgemuth S, Umezawa K, Mishina Y, Takaragi K. Competitive compliance with blockchain. In: 2019 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2019. Hitachi Ltd., Research Development Group, Kanazawa, Japan: Institute of Electrical and Electronics Engineers Inc.; 2019. p. 967–72. Available from: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067944621&doi=10.1109%2FPERCOMW.2019.8730684&partnerID=40&md5=96b9bb03111175586e8f94ee42f7dff6

24. Dolin RH, Boxwala A, Shalaby J. A pharmacogenomics clinical decision support service based on FHIR and CDS Hooks. Methods inf Med. 2018;57:e115–23. http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=emed19&NEWS=N&AN=625874890

25. Danahey K, Borden BA, Furner B, Yukman P, Hussain S, Saner D, et al. Simplifying the use of pharmacogenomics in clinical practice: building the genomic prescribing system. J Biomed Inf.2017;75:110–21. https://doi.org/10.1016/j.jbi.2017.09.012.

26. John SE, Channanath AM, Hebbar P, Nizam R, Thanaraj TA, Al-Mulla F. PharmaKU: A web-based tool aimed at improving outreach and clinical utility of pharmacogenomics. J Pers Med. 2021;11:210.

27. Linderman MD, McElroy L, Chang L. MySeq: privacy-protecting browser-based personal Genome analysis for genomics education and exploration. BMC Med Genomics. 2019;12:172. http://www.biomedcentral.com/bmcmedgenomics/

28. Gürsoy G, Brannon CM, Gerstein M. Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC Med Genomics. 2020;13:1–1.

29. Klein ME, Parvez MM, Shin JG. Clinical implementation of pharmacogenomics for personalized precision medicine: barriers and solutions. J Pharm Sci. 2017;106:2368–79.

30. Tata EB, Ambele MA, Pepper MS. Barriers to implementing clinical pharmacogenetics testing in sub-saharan africa. A critical review. Pharmaceutics 2020;12:1–19.

31. Rahma AT, Elbarazi I, Ali BR, Patrinos GP, Ahmed LA, Maskari FA. Genomics and pharmacogenomics knowledge, attitude and practice of pharmacists working in United Arab Emirates: Findings from focus group discussions—a qualitative study. J Pers Med. 2020;10:1–12.

32. Lee YM, Manzoor BS, Cavallari LH, Nutescu EA. Facilitators and barriers to the adoption of pharmacogenetic testing in an inner-city population. Pharmacotherapy. 2018;38:205–16.

33. Muflih S, Al-Husein BA, Karasneh R, Alzoubi KH. Physicians' attitudes and ethical obligations to pharmacogenetic testing. J Multidiscip Health. 2020;13:249.

34. Rafi I, Crinson I, Dawes M, Rafi D, Pirmohamed M, Walter FM. The implementation of pharmacogenomics into UK general practice: a qualitative study exploring barriers, challenges and opportunities. J Community Genet. 2020;11:269–77.

35. Hinderer M, Boerries M, Boeker M, Neumaier M, Loubal FP, Acker T, et al. Implementing pharmacogenomic clinical decision support into German hospitals. Stud Health Technol Inf. 2018;247:870–4.

36. McKillip RP, Galecki P, Ham S, Patrick-Miller L, Hall JP, Hussain S, et al. Patient (pt) perceptions of care as influenced by the implementation of a large institutional pharmacogenomic testing program. Clin Pharmacol Ther. 2016;99:S18–S18. http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=emed17&NEWS=N&AN=72216835

37. Longo C, Rahimzadeh V, O'doherty K, Bartlett G. Addressing ethical challenges at the intersection of pharmacogenomics and primary care using deliberative consultations. Pharmacogenomics. 2016;17:1795–805.

38. Rahma AT, Elbarazi I, Ali BR, Patrinos GP, Ahmed LA, Al-Maskari F. Stakeholders' interest and attitudes toward genomic medicine and pharmacogenomics implementation in the United Arab Emirates: a qualitative study. Public Health Genomics. 2021;24:99–109.

39. Bienfait K, Chhibber A, Marshall JC, Armstrong M, Cox C, Shaw PM, et al. Current challenges and opportunities for pharmacogenomics: Perspective of the Industry Pharmacogenomics Working Group (I-PWG). Hum. Genet. 2022;141:1165–73.

40. van der Wouden CH, Paasman E, Teichert M, Crone MR, Guchelaar H-J, Swen JJ. Assessing the implementation of pharmacogenomic panel-testing in primary care in the Netherlands utilizing a theoretical framework. J Clin Med. 2020;9:814.

41. Frigon MP, Blackburn MÈ, Dubois-Bouchard C, Gagnon AL, Tardif S, Tremblay K. Pharmacogenetic testing in primary care practice: opinions of physicians, pharmacists and patients. Pharmacogenomics. 2019;20:589–98.

42. Deininger KM, Tran JN, Tsunoda SM, Young GK, Lee YM, Anderson HD, et al. Stakeholder perspectives of the clinical utility of pharmacogenomic testing in solid organ transplantation. Pharmacogenomics. 2019;20:1291–302.

43. Alessandrini M, Chaudhry M, Dodgen TM, Pepper MS. Pharmacogenomics and global precision medicine in the context of adverse drug reactions: Top 10 opportunities and challenges for the next decade. Omi J Integr Biol. 2016;20:593–603.

44. Lemke AA, Selkirk CGH, Glaser NS, Sereika AWS, Wake DTW, Hulick PJ, et al. Primary care physician experiences with integrated pharmacogenomic testing in a community health system. Per Med. 2017;14:389–400.

45. Haga SB. Pharmacogenomic testing in pediatrics: Navigating the ethical, social, and legal challenges. Pharmgenomics Pers Med. 2019;12:273–85. https://www.dovepress.com/getfile.php?fileID=53273

46. Abou Diwan E, Zeitoun RI, Abou Haidar L, Cascorbi I, Khoueiry, Zgheib N. Implementation and obstacles of pharmacogenetics in clinical practice: an international survey. Br J Clin Pharmacol. 2019;85:2076–88.

47. Patel JN. Cancer pharmacogenomics, challenges in implementation, and patient-focused perspectives. Pharmgenomics Pers Med. 2016;9:65–77.

48. Luzum JA, Handelman SK, Pakyz RE, Palmer K, Shuldiner AR, Elsey AR, et al. The Pharmacogenomics Research Network Translational Pharmacogenetics Program: outcomes and metrics of pharmacogenetic implementations across diverse healthcare systems. Clin Pharmacol Ther. 2017;102:502–10. http://www.nature.com/clpt/index.html

49. Chang WC, Tanoshima R, Ross CJD. R, Carleton BC. Challenges and opportunities in implementing pharmacogenetic testing in clinical settings. Annu Rev Pharmacol Toxicol. 2021;61:65–84.

50. Sukasem C, Jantararoungtong T, Koomdee N. Pharmacogenomics research and its clinical implementation in Thailand: Lessons learned from the resource-limited settings. Drug Metab Pharmacokinet. 2021;39:100399.

51. Subasri M, Barrett D, Sibalija J, Bitacola L, Kim RB. Pharmacogenomic-based personalized medicine: Multistakeholder perspectives on implementational drivers and barriers in the Canadian healthcare system. Clin Transl Sci. 2021:cts.13083-cts.13083. https://onlinelibrary.wiley.com/doi/10.1111/cts.13083

52. Volpi S, Bult CJ, Chisholm RL, Deverka PA, Ginsburg GS, Jacob HJ, et al. Research directions in the clinical implementation of pharmacogenomics: an overview of US programs and projects. Clin Pharmacol Ther. 2018;103:778–86.

53. Martens FK, Rigter T, Cornel MC, Huntjens DW, Bet PM, Bartels M. DPD testing before treatment with fluoropyrimidines in the Amsterdam UMCs: an evaluation of current pharmacogenetic practice. Front Pharmacol. 2020;10:1609. http://www.frontiersin.org/Pharmacology

54. Bright D, Petry N, Roath E, Reckow E, Chavour S. Barriers, solutions, and effect of using pharmacogenomics data to support opioid prescribing. J Manag Care Spec Pharm. 2020;26:1597–602.

55. Cicali EJ, Weitzel KW, Elsey AR, Mosley S, Smith DM, Cavallari LH, et al. Challenges and lessons learned from clinical pharmacogenetic implementation of multiple gene-drug pairs across ambulatory care settings. Genet Med. 2019;21:2264–74. http://www.nature.com/gim/index.html

56. Milani L, Krebs K. Translating pharmacogenomics into clinical decisions: do not let the perfect be the enemy of the good. Hum Genomics. 2019;13:39. http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=emed20&NEWS=N&AN=629180467

57. Caraballo PJ, Hodge LS, Bielinski SJ, Stewart AK, Farrugia G, Schultz CG, et al. Multidisciplinary model to implement pharmacogenomics at the point of care. Genet Med. 2017;19:421–9.

58. Aifaoui A, Massmann A, Petry N, Hahn D, Baye J, Wilke RA, et al. Implementation of wide-scale pharmacogenetic testing in primary care. Pharmacogenomics. 2019;20:903–13. http://www.futuremedicine.com/loi/pgs?cookieSet=1

59. Haga SB. Integrating pharmacogenetic testing into primary care. Expert Rev Precis Med Drug Dev. 2017;2:327–36.

60. Lazaridis KN. PACE Forward-Making Pharmacogenomics Testing Available for Real-Life Clinical Utility. Clin Pharmacol Ther. 2018;105:42–4.

61. Rosenman MB, Decker B, Levy KD, Eadon MT, Holmes AM, Pratt VM. Lessons learned when introducing pharmacogenomic panel testing into clinical practice. Value Health. 2017;20:54–9. http://www.elsevier.com/wps/find/journaldescription.cws_home/724501/description#description

62. Etchegary H, Wilson B, Rahman P, Simmonds C, Pullman D. Public interest in whole genome sequencing and information needs: an online survey study. Per Med. 2020;17:283–93.

63. Patel JN. Cancer pharmacogenomics, challenges in implementation, and patient-focused perspectives. Pharmgenomics Pers. Med. 2016;9:65.

## AUTHOR CONTRIBUTIONS
FA and JHM conceived the article. FA drafted the article with input from JHM. All authors offered critical input and reviewed all drafts and agreed upon the final draft for submission.

## FUNDING

## COMPETING INTERESTS

The authors declare no competing interests.

## ADDITIONAL INFORMATION

**Supplementary information** The online version contains supplementary material available at https://doi.org/10.1038/s41397-022-00285-5.

**Correspondence** and requests for materials should be addressed to F. Albalwy.

**Reprints and permission information** is available at http://www.nature.com/reprints

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.